(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2003 (03.01.2003)

PCT

(10) International Publication Number
WO 03/001742 A1

(51) International Patent Classification[7]: H04L 12/28

(21) International Application Number: PCT/IL01/00577

(22) International Filing Date: 25 June 2001 (25.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **COMM-PRIZE VENTURES LIMITED** [GB/GB]; Sea Meadow House, Blackburne Highway, POB 116, Road Town, Tortola (VG).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **ALTMAN, Baruch** [IL/IL]; KKL Street 7, 37014 Pardes Hana (IL).

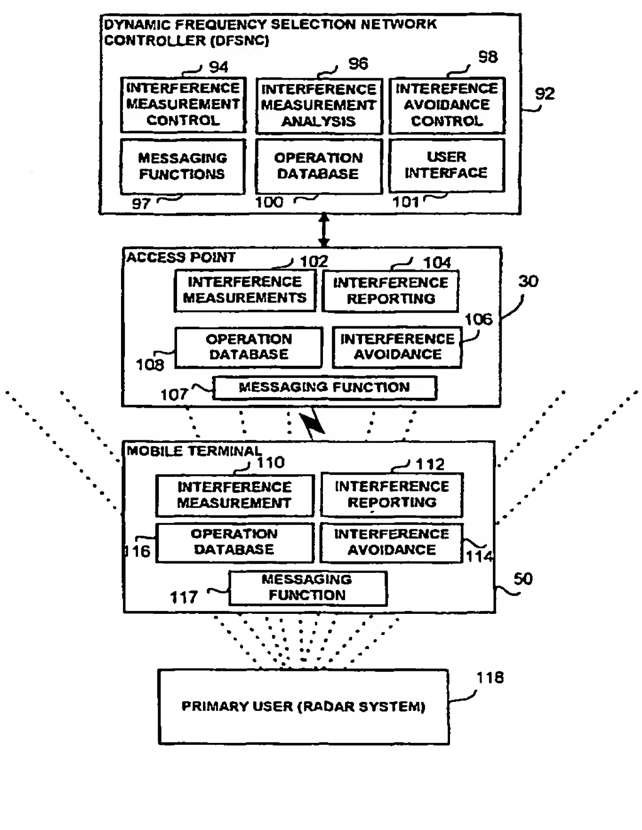
(74) Agents: **AGMON, Jonathan** et al.; Soroker - Agmon, Advocates and Patent Attorneys, 12th floor, Levinstein Tower, Petach Tikva Road, 66184 Tel Aviv (IL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR DETECTION OF AND DYNAMIC ADAPTATION TO RADIO INTERFERENCE IN A SHARED WIRELESS COMMUNICATIONS ENVIRONMENT



(57) Abstract: A method and system for interference detection and for dynamic adaptation and self-adjustment of a wireless communications system in response to the presence of an interfering signal in a communications channel. A controller device communicatively coupled to a network periodically instructs a device implemented in the wireless network to perform interference detection on one or more specified communications channels. The device performs the measurements, and returns the results to the controller. The controller analyzes the results, and determines the state of the measured channels in respect of the presence or the absence of a signal interference. Optionally interference avoidance measures are taken, such as switching the routine data transmission to a vacant communication channel, or utilizing the same channel co-operatively with the interfering signal. The avoidance measures could be implemented on a multi-network level, a single network level, a wireless transmitter level, or a directional sector level.

WO 03/001742 A1

Published:
— *with international search report*

METHOD AND SYSTEM FOR DETECTION OF AND DYNAMIC ADAPTATION TO RADIO INTERFERENCE IN A SHARED WIRELESS COMMUNICATIONS ENVIRONMENT

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The present invention relates to wireless communication systems in general, and to the dynamic detection and self-adjustment of the transmission parameters of a wireless local area network in response to prior controlled detection of radio frequency interference produced by diverse users, such as terrestrial radar, sky-borne radar, satellite transmitters, amateur radio service, or the like, sharing the same frequency band, in particular. The present invention further relates to a coexistence mechanism, which enables diverse radio frequency signal transceiving users to operate in parallel on the same frequency band.

DISCUSSION OF THE RELATED ART

The present invention offers a method and system for identifying signal interference phenomena produced by and applied reciprocally to wireless systems operating in a shared signal environment. The method and system is further operative in the prevention of the effects of the mutual interference to the wireless systems.

The regulating bodies dealing with the utilization of the radio frequency spectrum allocated certain frequency bands such that various wireless systems, such as wireless local area networks (WLANs), radar systems, satellite feeder systems, amateur radio services, and the like, may utilize simultaneously a shared range of frequencies. This commonality poses a strong potential for radio frequency interference in the shared communications environment. Interference occurs when a wireless device associated with a wireless data communications network, such as a WLAN, and a device associated with a another system, such as a radar, a satellite feeder, or a amateur radio transmitter, deployed in geographical

proximity or in effective broadcast range attempt to transmit substantially at the same point in time on the same frequency. In order to provide compatibility and ensure harmonic co-existence among the WLANs and the other systems operating in the same frequency band the regulating bodies attempted to mediate potential frequency conflicts by providing different priorities to different systems in the common band. Some systems, such as terrestrial radar, sky-borne radar, satellite feeders, amateur radio services, and the like, were designated as the "primary users" of the common band while other systems, such as WLANs, cellular phone networks, wireless personal area networks (WPANs), and the like, were designated as the "secondary users" of the same frequency band. The primary users were granted priority over the secondary users. It was further determined that the secondary users must not cause unacceptable interference to the primary users, and that the secondary users must accept all interference from the primary users. Thus, it is the responsibility of the secondary user, such as a WLAN, to avoid collision with a primary user, such as a radar system, a satellite transmitter, an amateur radio service, or the like. Consequently, the secondary user, such as a WLAN, must implement appropriate actions, such as detecting of the presence of an active primary user transmitting on a specific frequency within effective broadcast range, and avoiding transmission on the same frequency in order not to interfere with the primary user.

In an ideal world, timely information regarding radar system parameters, such as transmission frequencies, transmitting periods, and the like, would be routinely supplied to the operators of the functional WLANs to enable proper frequency planning of the wireless network. Such planning would provide the WLAN operators the capability of avoiding the use of frequencies associated with radar emissions, satellite broadcasts, amateur radio transmissions, and the like, in order to comply with regulations. In accordance with up-to-date information received about the activities and operational parameters of primary users deployed within effective range of one or more mobile terminals of a secondary user, such as a WLAN, the secondary user could be manually

pre-configured and periodically re-configured in order to refrain from transmitting on the frequencies utilized by the primary user.

In a realistic environment the situation is more complicated. In some countries for reasons of national security the parameters of certain primary users, such as military radar installations are not publicly available. The re-deployment of mobile radar installation for the duration of military exercises, or for periods of national emergency raises further difficulties. Occasionally transmitting, newly installed, or periodically re-configered primary user transmitters pose additional problems. Furthermore, primary users, such as radar systems, may occupy the bandwidth in a pseudo-random manner in respect to the portion of the bandwidth utilized, and to the bandwidth usage pattern. Thus, secondary users, such as WLANs, have to provide their own autonomous interference detection and avoidance means in order to avoid interference with such sensitive "partners" to the shared frequency band.

Currently, secondary users, such as WLANs, employ the "polling" technique for primary user interference detection. For example, at certain pre-defined points in time, such as at the WLAN system start-up, measurements are taken for the purpose of detecting active radar transmitters. The polling method may present difficulties when for various reasons the radar system is temporarily de-activated. For example, the radar transmitter can be shut down for the duration of maintenance activities or can be made periodically inoperative as a routine part of its standard operating procedure. When the points of time allocated by the WLAN for the performance of interference measurements coincide with or are included within the periods of the radar transmitter's inactivity the detection of the interfering transmission is not a viable option. Failure to detect activity could also be caused by the radar system operating in specific operational modes, such as in "sectorized" mode, where the radar scan is performed across a restricted azimuth range, or as in the "sweep" mode, where the radar scan is performed across the complete 360 degrees azimuth range. If the WLAN measurements period coincide with or contained in that segment rotational

periods during which the radar antenna radiation pattern is directed "away" from the measuring device then the transmission will not be detected.

Detection of a primary user transmission by a secondary user is also problematic due to physical issues, such as "interference asymmetry". Typically, primary users, such as radar systems, do not interfere "significantly enough" with secondary users, such as a WLAN, compared with the interference effected to a primary user, such as a radar system, by the transmission of signals from WLAN devices and reception of the signals by the receiver of a radar system. Due to the longer distances covered by the radar signals (the radar signals may travel a path from the radar transmitter to a reflecting target, and back to a WLAN receiver) in respect to the distance covered by the WLAN signals (typically, half the distance of the radar signals as the WLAN signal path includes single route segment between a WLAN transmitter to a radar receiver), and the resulting asymmetry in the respective propagation losses, the primary user is more interfered with by the WLAN than the WLAN is interfered by the primary user. Furthermore the radar system is more sensitive to interference due to differences in the system-specific modulation techniques. Similar interference asymmetry-related problems may also exist in regard to an interference involving a WLAN and other types of primary users, such as satellite transmitters, amateur radio service, or the like, as well.

WLAN devices are capable of detecting the presence of interfering transmitters and taking suitable actions for the avoidance of mutual signal interference by moving to an unused communication channel. The channel switch is accomplished through the utilization of a set of functions typically referred to as the Dynamic Frequency Selection (DFS) or as the Dynamic Channel Selection (DCS). In the text of this document the DFS acronym will be used.

DFS is a vendor-specific mechanism, without established and published standards but the general principles are known. Currently, the DFS function is mainly based on received signal strength (idle channel RSS) measurement taken during WLAN-idle channel conditions. Access Point (AP)

devices utilized as bridges between a wired and a wireless local area network make the measurements themselves or can require the Mobile Terminals (MT) linked thereto to take the measurements. The measurements can be taken on a channel in use or on another frequency. Interfering signals can be detected by measuring the received signal strength at intervals within a specified time slot and comparing the result to a predefined threshold value. If the idle channel RSS is higher than a maximum allowed value then it can be concluded that a strong interference source, such as a radar transmitter operates in the vicinity.

Co-existence is defined as the ability of a system to perform a task in a shared environment where other systems may or may not be using the same set of rules. Multiple wireless devices are said to co-exist if they can be collocated without significantly impacting the performance of these devices. Providing a co-existence mechanism among secondary users, such as WLANs, and primary users, such as radar systems, is important for the better utilization of the radio frequency spectrum, which is a scarce, costly, and therefore a heavily regulated resource. When signals emitted from a periodic radar transmitter associated with a pulse or sweep radar system are detected by the WLAN in respect to a specific communication channel with an allocated specific frequency, the WLAN takes suitable interference countermeasures such as moving to a vacant channel within its own allocated frequency band. The technique has a drawback such that it is substantially wasteful in terms of the useable bandwidth and in terms of WLAN-performance efficiency. It would be preferable for the WLAN to keep using the channel interfered with and co-exist with the interfering signal.

It would be readily perceived that there is an urgent need for a method and system for the detection of diverse primary users, such as non-pre-configured radar systems by secondary users, such as WLAN's, in a signal environment shared by both systems. There is also a clear and present need for a method and system to provide an improved utilization of the bandwidth available to a wireless communications system by providing a mechanism that enables co-existence of a primary user, such as a radar system, satellite system, amateur radio service, and

the like, and a secondary user, such as a WLAN, where both systems operate on a shared frequency band.

SUMMARY OF THE PRESENT INVENTION

One aspect of the present invention regards a wireless communications environment accommodating at least one secondary user transmitting and receiving a radio frequency signal on an allocated frequency band, at least one primary user transmitting and receiving a radio frequency signal on a substantially alike allocated frequency band, and a method for the detecting and avoiding reciprocal signal interference produced by the radiation of the radio frequency signals emitted by the at least one primary user and by the at least one secondary user. The method includes establishing and dynamically maintaining interference detection and avoidance control and operation information in the at least one secondary user, dynamically and controllably measuring at least one communication channel providing a communication path between at least two wireless devices of the at least one secondary user, analyzing the results of measurements performed on the at least one communications channel in order to determine the interference status of the measured at least one communications channel of the at least one secondary user, dynamically maintaining interference detection and avoidance information in the at least one secondary user, and selectively and controllably performing interference avoidance procedures by the at least one secondary user to prevent reciprocal signal interference in the at least one secondary user and in the at least one primary user.

A second aspect of the present invention regards a communication environment accommodating at least one secondary user transmitting and receiving a radio frequency signal on an allocated frequency band via a wireless or wired link, at least one primary user transmitting and receiving a radio frequency signal on a substantially same allocated frequency band via an unbounded medium, and a system for the dynamic detection of reciprocal signal

interference produced substantially simultaneously by the at least one secondary user and at least one primary user. The system contains at least one primary user interference detection and avoidance controller device, and at least one primary user interference detection and avoidance wireless device.

A third aspect of the present invention regards a wireless communications environment accommodating at least one secondary user transmitting and receiving a radio frequency signal on a allocated frequency band via an air interface, at least one primary user transmitting and receiving a radio frequency signal on a substantially alike allocated frequency band via an air interface, and a method of detecting and avoiding signal interference effected to the at least one primary user by the transmission of the signal emitted by the at least one secondary user. The method includes the steps of dynamically and controllably measuring at least one communications channel utilized the at least one primary user, analyzing the results of the channel measurements performed on the at least one communications channel utilized by the at least one primary user in order to determine the interference status of the measured channel, communicating the results of the analysis to the at least one secondary user interference detection and avoidance controller device, dynamically maintaining interference detection and avoidance information concerning the identity, attributes, locations, directionality, and activity of at least one wireless device associated with at least one secondary user interfering with the at least one measured communications channel associated with the at least one primary user, and selectively and controllably performing interference avoidance measures by the at least one secondary user interference detection and avoidance controller device to prevent signal interference in the at least one communications channel associated with the at least one primary user.

A fourth aspect of the present invention regards a communication environment accommodating at least one secondary user transmitting and receiving a radio frequency signal on allocated frequency band via a wireless or wired link, at least one primary user transmitting and receiving a radio frequency

signal on a substantially same allocated frequency band via an unbounded medium, and a system for the dynamic detection of reciprocal signal interference produced substantially simultaneously by the at least one secondary user and at least one primary user. The system consists of at least one primary user interference detection and avoidance controller device to communicate with and control at least one secondary user activity detection wireless device, and at least one secondary user activity detection wireless device to perform measurements on at least one communication channel utilized by the primary user in order to detect interference produced by the activity of at least one secondary user.

All the above aspects of the present invention provide for the dynamic and controlled detection of a radio frequency signal interference in a secondary user operating in a wireless signal environment.

All the above aspects of the present invention provide for the dynamic and controlled detection of a radio frequency signal interference in a primary user operating in a wireless signal environment.

All the above aspects of the present invention provide for the dynamically and adaptively adjust the transmission parameters of a secondary user operating in a shared signal environment.

All the above aspects of the present invention provide for preventing reciprocal signal interference in a secondary user and in a primary user by utilizing alternative interference avoidance schemes.

All the above aspects of the present invention enable co-existence of an active secondary user and an active primary user on a substantially same communications channel.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description taken in conjunction with the drawings in which:

Fig. 1 is a schematic block diagram of a wireless communications environment as known in the art; and

Fig. 2 is a block diagram of an HiperLAN/2 protocol architecture as implemented in a mobile terminal associated with a wireless communications network as known in the art; and

Fig. 3 illustrates the basic Medium Access Control (MAC) frame structure associated with the HiperLAN/2 protocol architecture as known in the art; and

Fig. 4 is a schematic block diagram illustrating an exemplary configuration of the proposed system, in accordance with the preferred embodiment of the present invention; and

Fig. 4A is a schematic block diagram illustrating an exemplary alternative configuration of the proposed system, in accordance with the preferred embodiment of the present invention; and

Fig. 5 is block diagram illustrates an exemplary configuration including a detailed view of the operative components associated with the proposed system, in accordance with the preferred embodiment of the present invention; and

Fig. 6 is a schematic block diagram showing the various tables constituting an exemplary operation database, in accordance with a preferred embodiment of the present invention; and

Fig. 7 is a flow chart depicting an exemplary set of operational steps involved in the performance of interference detection in the DFSNC control mode, in accordance with the first preferred embodiment of the present invention; and

Fig. 8 is a flow chart showing an exemplary set of operations involved in the performance of the interference detection in the wireless device control mode, in accordance with a second preferred embodiment of the present invention; and

Fig. 9 is a flow chart depicting an exemplary set of operational steps involved in the performance of he interference detection in the pattern recognition based interference detection mode, in accordance with a third preferred embodiment of the present invention; and

Fig. 10 is a flow chart depicting an exemplary set of operational steps involved in the performance of the interference detection in the co-existence mode, in accordance with a fourth preferred embodiment of the present invention; and

Fig. 11 is a graphical representation of an exemplary signals collision in a specific WLAN channel and an exemplary frequency re-assignment based solution to the conflict, in accordance to the first, second, and third embodiment of the present invention; and

Fig. 12 is a graphical representation of an exemplary signal collision in a specific WLAN channel and of the exemplary co-existence option based solution to the conflict, in accordance with the fourth embodiment of the present invention; and

Fig. 13 is an block diagram illustrating the operation of an exemplary sectorized detector Access Point device, in accordance with the fifth preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

A method and system for remote interference detection and for dynamic adaptation of the operation of a wireless communications network in response to the state of the communications channels thereof affected by the presence of interfering signals in the channels is disclosed. A wireless communications network operating in a shared frequency band dynamically detects interference caused by a primary user, such as a radar system, by controllably taking measurements of one or more communication channels.

The method and system of the present invention are disclosed through the detailed description of several preferred embodiments. The embodiments can be implemented separately or in any functional combination appropriate to the implementation of the proposed system. In the first preferred embodiment of the present invention, the system operates in a specific operational mode, referred to as the DFSNC control mode. A controller device communicatively coupled to the wireless network and having an operation database established therein, periodically submits requests associated with a set of functional parameters held in the operation database to an access point and/or a mobile terminal communicatively linked to the same wireless network in order to perform communications channel measurements. The purpose of the measurements is the detection of the activity of a primary user operating in the same signal environment. The access point and/or the mobile terminal collects the requested channel measurement results produced according to the set of the functional parameters transmitted by the controller device and returns the measurement values obtained to the controller device. The controller device analyses the results of the channel measurement values received from the access point and/or mobile terminal, and in accordance with the products of the analysis and of a predetermined set of rules and data, determines the presence and optionally the power level of an interfering signal generated by the activity of a primary user on the measured communication channel. If a primary user-related interfering signal is detected then, in accordance with the current signal measurement results, the

prior signal measurement results, and a predefined set of data in rules in the operation database, the controller device could instruct the access point and/or mobile terminal to take suitable interference avoidance measures, such as moving to a vacant communication channel within the allocated frequency range, lowering the transmission power, or activating a specific co-existence mechanism. Additionally the controller device updates the operation database with essential information concerning the values of the channel measurements and the products of the analysis process. Subsequently the controller device alerts the network controller and/or the network operators. The controller device may further utilize the results of the analysis as a trigger to issue a set of instructions to other wireless networks, which are known to operate in the environment and are known to utilize the channel being interfered with.

The second preferred embodiment of the present invention the system operates in a specific operational mode referred to as the wireless device control mode. The controller device according to instructions of a network operator downloads a set of parameters functional to the performance of the primary user-related interference detection scheme to an access point and/or a mobile terminal. The downloaded parameters are stored within an operation database established in the access point and/or the mobile terminal. The periodic execution of the interference detection process is performed by the access point and/or the mobile terminal independently of the controller device, and according to the parameter values received from the controller device. The analysis of the channel measurement values, the determination regarding the presence and optionally the power level of an interfering signal generated by a primary user on the measured communications channel, and the necessary actions to be taken, such as channel re-assignments, transmission power adjustments, or co-existence handling, are executed by the access point and/or the mobile terminal and/or the controller device. The access point and/or the mobile terminal update the operation database established therein and optionally upload the essential update information to the controller device.

The third preferred embodiment of the present invention the system operates in a specific operational mode referred to as the pattern-recognition-based interference detection mode. A predefined interference pattern table and a channel parameter table is established on the access point and/or the mobile terminal deployed within the wireless network. In the course of the routine data exchange operations the access point and/or the mobile terminal collects changes sequentially occurring in the standard channel parameters, such as bit error rates, frame error rates, or the like. Additional changes to be collected can be physical layer parameters, such as symbol error rate, mean distance of correlation, mean error of the frequency/phase/amplitude modulation, and the like. The changes in the channel parameters are obtained continuously during any routine data exchanges, such as between the access point and the mobile terminal, or as between different mobile terminals. The changes are recorded in the channel parameter changes table. Then the changes are selectively analyzed in order to detect certain meaningful patterns. When the certain meaningful patterns are detected the access point and/or the mobile terminal and/or the controller device could initiate appropriate interference avoidance techniques, such as moving to a vacant channel within the allocated frequency range, adjusting the transmission power, or activating the co-existence mechanism. Additionally the access point and/or the mobile terminal update the local operation database, optionally upload essential information to the remote network controller concerning the results of the pattern-recognition-based interference detection scheme, and suitably notify the controller device regarding the consequent actions taken. In the third preferred embodiment of the present invention, interference detection is performed by the access point and/or the mobile terminal as an integral part of the normal operation of the wireless device.

In the fourth preferred embodiment of the present invention the system operates in a specific operational mode, referred to as the Detector Device mode. A detector device is a wireless platform co-located with a known primary user, such as a radar system, at the known primary user site, such as a radar

installation. The detector device is coupled to the controller of a wireless communications network via a wireless or a wired link. The detector device is used to detect wireless activity that could interfere with the operation of the primary user. The detector device could further be programmed to collect and store the vital transmission parameters of the primary user, such as the transmission channel, the transmission periods, transmission/reception coverage areas, and the like. This information could be also provided to the detector device by the network operator via a suitable user interface. The detector device is operative in scanning the transmission channel that is known to be used by the primary user for the purpose of detecting wireless communications network transmissions on the same channel such that the transmission could have a significant impact on the performance of the primary user. Subsequent to the detection of such activity the detector device alerts the controller device of the transmitting wireless network. The alert may further include significant control information, such as the network identification, access point identification, transmitting device identification, the periods of the transmission, and the like. The information may also include the transmission parameters of the primary user. In accordance with the received alert and the attached information the wireless network controller identifies the transmitting individual device and may instruct the device to take appropriate interference avoidance measures, such as switching channels, cease transmitting, or suitably adjusting the power level of the transmission.

The detector device could be sectorized. When sectorized the detector device could collect, collate and communicate information having a directional dimension. The information communicated could be based on a RF topology mapping of the signal environment including the location and the permanent or temporary directionality of a primary user and the location of the sectorized or non-sectorized WLAN devices with their existing sectors and sectors' directions. The map could be created manually by a network operator and/or by appropriate interference detection-driven modules implemented on the detector device. The

additional directional information could enable the detector device to control the interference avoidance measures taken by the WLAN devices on a sector level. Thus, a sectorized WLAN device could be instructed to take suitable interference avoidance measures, such as "going silent" on one or more of its sectors, lowering power levels on one or more of its sectors while keep transmitting normally on the rest of its sectors.

Subsequent to the detection of a primary user-related interference alternative interference avoidance schemes can be performed. The interference avoidance measures include but are not limited to channel re-assignment, transmission power adjustment, and the activation of a co-existence mechanism. Alternative interference detection modes can be used in various combinations with the proposed interference avoidance measures. Channel switching and the adjustment of the signal power levels are known techniques. The co-existence mechanism involves the establishment of an interfering signal periodicity table, and a time window table on the access point and/or the mobile terminal and/or the controller device deployed within the wireless network. The tables could be built and maintained by a network operator according to known information concerning the activities of a known primary user in the environment. The tables could also be created and maintained automatically by the access point and/or the mobile terminal and/or the controller device through the utilization of an interference detection scheme. The tables are examined by the access point and/or the mobile terminal and/or the controller in respect to the temporal regularity of the interfering signal in order to determine the interfering signal transmission periods. If periodicity of the interfering signal is established then the co-existence mechanism may be activated. A time window control table is set up on the access point and/or the mobile terminal and/or the controller device. The time window control table is operative in providing time slots specific to the transmission periods of the interfering signal. In these established primary user-specific time slots the entire wireless network i.e., the access points and the mobile terminals thereof, is instructed not to transmit or to lower the transmission power level in

order not to interfere with the primary user's signal. Consequently, the access point and/or the mobile terminal may keep operating on the same channel. By providing the channel periodic silent periods or reduced level of transmission the wireless network avoids interference with the established primary user's signal and thereby achieves co-existence with the primary user.

In the preferred embodiments of the present invention the secondary user is a wireless communication network, and more specifically a wireless local area network (WLAN). The primary user of the shared communications band is a radar system. It would be clear to one with ordinary skills in the art that in other preferred embodiments of the present invention diverse other wireless communications network could be used such as cellular telephone systems, wireless personal area networks, and the like. The primary user of the shared frequency band could be any other transmitting source designated as the system having priority in the utilization of the allocated frequency band, such as Industrial, Scientific, and Medical (ISM) devices, amateur radio services, terrestrial or sky-borne radar systems, satellite feeders, or the like. In the preferred embodiment of the present invention the mobile terminal referred to is a laptop computer, such as a ThinkPad 360 of IBM, a 4000 CT of HP, or the like. The mobile terminal could also be a stand-alone wireless station such as a modem card, or the like. In other preferred embodiments of the invention diverse other devices could be used such as cellular phones, Personal Digital Assistants (PDAs), and the like. The following description is provided to enable a ready understanding of the operations and the functional structure of the system proposed by the present invention and not meant to be limiting such as to exclude diverse other uses that could be contemplated, developed, and based on the underlying concept of the present invention. The scope of the invention is to be limited only by the attached claims.

According to the practices of persons skilled in the art of computer programming, the present invention is described below with reference to actions and symbolic representations of operations that are performed by the processing

computer system. It will be readily understood by one skilled in the art that the actions and the symbolically represented operations include the manipulation of electric signals by a central processing unit (CPU). The electrical signals represent data bits which effect a resulting transformation or reduction of the electrical signal representation, and the maintenance of data bits at memory locations in the memory system to thereby reconfigure or otherwise alter he CPU's operation, as well as other processing of signals. The memory locations are physical locations that have particular electrical, magnetic, or optical, properties corresponding to the data bits. The interference detection and avoidance method includes sets of computer programs implemented on different computing and communicating platforms and consisting of computer software instructions specifically developed for the practice of the present invention. The software installed in the network controller, in the access points, and the mobile terminals causes the controller, the access points, and the mobile terminals respectively to perform the various functions described herein. In the preferred embodiments of the present invention dedicated electronic hardware is made and used to perform all functionality described herein. The interference detection and avoidance method is implemented as firmware by the embedding of the predetermined program instructions and/or appropriate control information and associated data within suitable electronic hardware devices containing application-specific integrated circuits (ASIC).

Referring now to Fig. 1 that illustrates a communications environment in which the preferred embodiments of the present invention can operate. Fig. 1 is illustrative only and it is not the only communications environment in which the various preferred embodiments of the present invention can operate. The environment contains a wired network 10, a wireless network 20, a wireless network 21, a wireless network 23, and a primary user, such as a radar system 62. Wired network 10 is coupled to wireless network 20 via standard communication lines 22, 24, 26, and via link 27. Specific activities of the wireless network 21 and

the wireless network 23 can be controlled by the communication of information from wireless network 20. Therefore, the network 21 and the network 23 are communicatively linked to the wireless network 20 via a link 25', and a link 25'' respectively. Although in the drawing only two wireless networks are shown it would be easily understood that in a realistically configured environment several wireless networks could be coupled to the network 20. Wired network 10 is a Local Area Computer Network (LAN) that includes various computing and communicating devices such as a network manager 14, a network printer 16, and a network terminal 18 linked by fixed communication lines such as one or more coaxial cables, twisted pair, fiber optics, and any other media to support wired communications. In another preferred embodiments a wireless communication network can replace the wired network 10. In yet other embodiments wired network 10 can be a Wide Area Network (WAN). Although in the drawing only three wired network devices are shown it would be easily understood that in a realistically configured wired network a plurality of devices could operate. Network manager 14 includes a computing platform such as a Personal Computer (PC), a Sun workstation, a MacIntosh computer, or a specialized network management device. The network manager 14 includes a memory for storing information and a process for accessing and processing the information. Wired network 10 is linked to Access Points (AP) 28, 30, 32 via respective communication lines 22, 24, 26. AP devices 28, 30, 32 include a computing and communication platform. The function of the Access Points is to bridge traffic from the wired network infrastructure 10 to the mobile terminals. Lines 22, 24, 26 include one or more coaxial cables, twisted pair, fiber optics or any other media to support wired communication. Each AP includes a transceiver (not shown) to support wireless communication and a Dynamic Frequency Selection component (DFS) 34, 36, and 38 to support interference detection and avoidance. The network 10 is communicatively connected to a wireless access point (AP) 31 via a link 27. The AP 31 includes a transceiver (not shown) to support wireless communication and a DFS 33 to support interference detection and avoidance.

The AP 28, 30, 31, 32 are communicatively linked to one or more mobile terminals (MT) 40, 42, 44, 46, 50 via links. Each MT includes a transceiver (not shown) supporting wireless communication and a DFS to support interference detection and avoidance. The AP 28, 30, 31, 32 are controlled by a network manager device 14 and communicate with the MT 40, 42, 44, 46, 50 through radio frequency signals transmitted by their respective transceivers. The primary user of the designated frequency band, such as the radar system 62, functions in the communications environment through the transmission of a continuous or a periodic radio frequency signal typically in the microwave band of the spectrum. It is undesirable that the signals emitted by the radar system 62 received by the wireless networks 20, 21, and 23, as the radar signal will interfere with the WLAN signals. Nevertheless if one or more wireless devices deployed within the wireless networks 20, 21, 23 are in the operational range of the radar system's 62 transmitter the wireless devices may receive the radar signal. The unintended reception of the radar signal will effect interference with the radio frequency signals communicated between the AP devices 28, 30, 31, 32 and the MT devices 40, 42, 44, 46, 50. Similarly the radio frequency signals communicated by the transmitting devices of the WLAN 20, 21, 23 could interfere with the reflected radar signal received by the radar system 62. Such interference could degrade the quality of the communication within the WLAN 20, 21, 23 and could jam the signals transmitted by the radar system 62 and thus cause it to malfunction. Note should be taken that networks 20, 21, and 23 could be deployed in different distances and different directions from the radar system 62. Thus, the strength and the directionality of the signals effecting mutual interference between each of the networks 20, 21, 23 and the radar system 62 could be varied. Note should be also taken that the function of the DFS components 34, 36, 38, 33, 52, 54, 56, 58, 60 is to attempt to minimize the effects of interference between the various inter-network devices, and between devices of different wireless network devices, such as Bluetooth devices, cellular devices, and the like.

In the preferred embodiments of the present invention, the WLAN 20 of Fig. 1 is a HiperLAN/2-type wireless network. HiperLAN/2 is a broadband radio transmission technology operating in the 5 GHz frequency band. Currently frequencies are allocated for HiperLAN networks within in the 5.15-5.825 GHz band depending on geographical area in which the network is implemented. In other embodiments of the present invention alternative technologies could be used such as 802.11a, 802.11h, HiperLAN, OpenAir, HomeRF, HiSWAN (Japan), or the like. The features of the HiperLAN/2 standard are known. In order to enable ready understanding of the method and system suggested by the present invention, a brief and simplified description will be provided concerning the protocol architecture of the HiperLAN/2 radio interface as implemented for a mobile terminal associated with the WLAN 20 of Fig. 1, and the Medium Access Control (MAC) frame structure. The description will deal with those parts of the protocol and the MAC frame that are relevant to the method and system proposed by the present invention.

Referring now to Fig. 2 illustrating the implementation of the HiperLAN/2 protocol stack in a mobile terminal (MT) 81. Using OSI 7 layers model as the reference model, the MT device 81 operates within a WLAN and is communicatively linked to a wired LAN via one or more Access Points (AP) that bridge the WLAN with a wired LAN. The MT 81 includes a Physical Layer (PHY) 90, and a Data Link Control Layer (DLC) 82. The MT 81 could also include transport channels 89, and Convergence Layer (CL) 83. The sub-layer functions as detailed below are of the HiperLAN/2 protocol. In other protocols certain functions may or may not exist, other functions could be added or removed, and the division of the sub-functionality may differ. The PHY 90 supports the electrical or mechanical interface to the physical medium. For example, this layer determines how to put a stream of bits from the DLC layer 82 on to a radio carrier. The physical layer is usually a combination of software and hardware programming and may include electromechanical devices. The functions

of the CL 83 is adapting service requests from the higher protocol layers to the service offered by the DLC 82, and to convert the higher level data packets into a fixed size that is used within the DLC 82. The DLC 82 constitutes the logical link between an Access Point (AP) and the mobile terminal (MT) 81. The DLC 82 assures that an initial connection has been set up, divides output data into data frames, and handles the acknowledgements from a receiver that the data arrived successfully. It also ensures that incoming data has been received successfully by analyzing bit patterns at special places in the frames. The DLC 82 includes functions for medium access and transmission as well as terminal and connection handling. Thus the DLC 82 layer consists of a set of sub-layers: a Medium Access Control (MAC) protocol 88, an Error Control (EC) protocol 86, and a Radio Link Control (RLC) protocol 84. The MAC protocol 88 is used for access to the radio link with the resulting transmission of data onto that medium. EC protocol 86 is used to increase reliability over the radio link by detecting bit errors and re-transmitting the data if such errors are detected. EC 86 also ensures that the data units are delivered in-sequence to the CL 83. RLC 84 gives a transport service to the signaling entities such as Association Control Function (ACF) 95, Radio Resource Control function (RRC) 92, and the Connection Control Function (CCF) 96. RLC 84, ACF 95, RRC 94 and CCF 96 provide for the exchange of signaling messages between an Access Point (AP) and the MT 81. RRC 92 is a group of control functions on the top of the RLC 84 that is responsible for the handling of the radio resources. RRC 92 includes a Dynamic Frequency Selection (DFS) function 94 to provide for the performance of measurements on radio signals received from neighboring mobile terminals as well as to instruct the MT 81 to perform measurements when needed. Subsequently the DFS 94 automatically allocates vacant frequencies to each AP for communication, allows several operators to share the available frequency spectrum, and can be used to avoid the use of interfered frequencies. Note should be taken that the DFS 94 sub-function need not necessarily be part of the RRC 94. RRC 94 could be an independent function or could be embedded within a different sub-functionality.

The air interface in HiperLAN/2 is based on time-division duplex (TTD) and dynamic time-division multiple access (TDMA) methods. The time-slotted structure of the medium allows for simultaneous communications in both downlink and uplink within the same time frame called MAC frame. Time slots for downlink and uplink communication are allocated dynamically depending on the need for transmission resources. The basic MAC frame on the air interface has a fixed duration of 2 ms and comprises transport channels for broadcast control, frame control, access control, downlink (DL) and uplink (UL) data transmission and random access. The MAC frame and the transport channels form the interface between DLC 82 and the PHY 90.

Referring now to Fig. 3 illustrating the basic MAC frame structure. MAC frames 200, 201, 202 each comprise broadcast channel (BCH) 203, frame control channel (FCH) 204, access feedback channel (ACH) 205, DL phase 205, and a UL phase 206, and random access channel 207. The BCH 203 contains control information sent in every MAC frame and reaches all the MTs, such as transmission power levels, AP identifiers, network identifiers, and the like. The FCH 204 contains a description of the resources allocated within the current MAC frame. The ACH 205 conveys information on previous access attempts made in the RCH. Downlink and uplink traffic (DL 206 and UL 207) consist of Protocol Data Unit (PDU) trains to and from the MTs. The RCH 208 is used by the MTs to request transmission resources for the DL phase 206 and the UL phase 207 in the upcoming MAC frames and convey the RLC 84 signaling messages.

Fig. 4 illustrates the components constituting the proposed system and functional to the operation of the proposed method of the present invention. The illustrated configuration is exemplary only and in order to accomplish the objectives of the proposed method and system various other configurations could be used. The method involves the exchange of a plurality of downloaded and uploaded messages between the mobile terminals of the WLAN and a remote

interference detection controller. In addition to the standard data exchange packets the messages include but are not limited to instructions with associated parameters, notifications, requests, replies, reports, measurement parameters such as threshold values, measurement results, range of blocked channels, range of channels to operate with, neighboring channels allocated, operation instructions, and the like. The operation instructions include but are not limited to ceasing transmission in one or more specific sectors, to provide re-adjusting the transmission power of other specific sectors, to increase permanently or temporarily the time allocation to specific sectors, and the like. The WLAN 20 is communicatively coupled to a wireless network 21 and a wireless network 23 via the links 25 and 27 respectively. The WLAN 20 is operative in communicating interference detection information to networks 21, and 23 in order to enable networks 21, 23 to take appropriate interference avoidance measures. Networks 21, and 23 could also communicate relevant information to network 20. The WLAN 20 includes a remote Dynamic Frequency Selection Network Controller (DFSNC) 92, an AP 30 and a MT 44. The DFSNC 92 could be co-located with the AP 30, or with an another AP (not shown) deployed within the network and thus is remote to the set of APs deployed within the network The DFSNC 92 could be also a stand-alone device. The DFSNC 92 includes a computing and communication platform such as a PC and is connected to the AP 30 via a link 24. The DFSNC 92 could include a transceiver (not shown) to support wireless communication. The function of the DFSNC 92 is to control remotely interference detection and avoidance by communicating with the AP 30 and the MT 44. The AP 30 is coupled to the MT 44 via a link 101. Although only one DFSNC, one AP and one MT are shown on the drawing discussed it is understood that a realistically configured network could contain more than one DFSNC and more than one AP devices coupled communicatively to one more MT devices. The AP 30 includes a transceiver (not shown) to support wireless communication and a set of DFS functions 36 to support interference detection and avoidance. The MT 44 includes a transceiver (not shown) to support wireless communication and a

set of DFS functions 56 to support interference detection and avoidance. Periodically, according to pre-defined operational parameters introduced by a WLAN operator, the DFSNC 92 sends suitable instructions via the link 24 to AP 30 and to MT 44 to initiate interference detection. The instruction includes parameters operative in defining the type of detection to be performed, the measurements to be collected, the channel to be measured, the sub-set of potentially usable channels, and the like. Consequently the AP 30 and/or the MT 44 perform the required measurements by utilizing the set of DFS functions 36 and the set of DFS functions 56 respectively. The AP 30 could perform the measurements itself or could instruct the MT 44 to via the link 101 to perform the same. The results of the detection process are returned by the MT 44 and/or by the AP 30 to the DFSNC 92 for analysis. The DFSNC 92 performs the analysis on the results received. The products of the analysis provide information concerning the presence, the absence, and the power level of an interfering signal on a specifically measured channel. When a primary user-generated interference is identified by the DFSNC 92 an instruction is sent from the DFSNC 92 via the link 24 to the AP 30 and/or to the MT 44 regarding the activation of the set of the DFS functions 36 and the set of DFS functions 56 respectively in order to take appropriate interference avoidance measures, such as moving to another channel within the allocated frequency band of the WLAN 20.

Fig. 4A illustrates alternative configuration of the proposed system that is functional to the operation of the proposed method of the present invention. The illustrated configuration is exemplary only and in order to accomplish the objectives of the proposed method and system various other configurations could be used. The WLAN 20 is communicatively coupled to the wireless networks 21 and 23 via links 25, and 27 respectively. The WLAN 20 is operative in communicating interference detection alerts and associated information to networks 21, 23. Similarly, networks 21 and 23 communicate relevant information, such as topology data, identified primary users, and the like, back to

WLAN 20. The WLAN 20 includes a remote Dynamic Frequency Selection Network Controller (DFSNC) 92, and a MT 44. The DFSNC 92 includes a computing and communication platform such as a PC and is connected to the MT 44 via a link 24. The DFSNC 92 may include a transceiver (not shown) to support wireless communication. The function of the DFSNC 92 is to control remotely interference detection and avoidance by communicating with the MT 44. Although only one DFSNC and one MT are shown on the drawing discussed it is understood that a realistically configured network could contain more than one DFSNC coupled communicatively to one or more MT devices. The MT 44 includes a transceiver (not shown) to support wireless communication and a set of DFS functions 56 to support interference detection and avoidance. Periodically, according to pre-defined operational parameters introduced by a WLAN operator, the DFSNC 92 sends suitable instructions via the link 24 to MT 44 to initiate interference detection. The instruction includes parameters operative in defining the type of detection to be performed, the measurements to be collected, the channel to be measured, the sub-set of a potentially usable channels, and the like. Consequently the MT 44 perform the required measurements by utilizing the set of DFS functions 56. The results of the detection process are returned by the MT 44 to the DFSNC 92 for analysis. The DFSNC 92 performs the analysis on the results received. The products of the analysis provide information concerning the presence, the absence, and the power level of an interfering signal on a specifically measured channel. When such an interference is identified by the DFSNC 92 an instruction is downloaded from the DFSNC 92 via the link 24 to the MT 44 regarding the activation of the set of DFS functions 56 in order to take appropriate interference avoidance measures, such as moving to another channel within the allocated frequency band of the WLAN 20. Note should be taken in the above-described configuration no AP device is implemented. Therefore all the functionalities of the AP are implemented in the MT 44 as access point functionality 55.

Fig. 5 provides a detailed view of the operative components associated with the proposed method and system. The illustrated configuration is exemplary only and in order to accomplish the objectives of the proposed method and system various other configurations could be used. The exemplary system configuration presented consists of a remote DFSNC 92, an AP 30, and a MT 50. A primary user device 118 is an interfering source, which is operating near to the WLAN and transmitting radio frequency signals. In the preferred embodiment of the present invention the primary user device 118 is a radar transmitter. The DFSNC 92 is programmable device. The DFSNC is pre-configured and can be periodically re-configured by the network operator utilizing the user interface 101. The re-configuration is effected by the manipulation of the relevant data stored in the operation database 100. Although only one DFSNC is shown on the drawing under discussion more than one such devices could be deployed across the wireless network space when each separate device could be programmed and configured in a different manner according to the network topography, known local interference sources, and the like. The DFSNC 92 is dynamically configured according to the results of the interference detection process performed by the AP 30 and/or the MT 50. The DFSNC 92 is capable of controlling a distinct sub-set of mobile terminals in the network or the entire set of mobile terminals deployed across the WLAN space. The DFSNC 92 includes but not limited to a user interface 101, an interference measurement control 94, an interference measurement analysis 96, an interference avoidance control 98, a messaging function 97, and an operation database 100. The operation database 100 is pre-configured by the wireless network operator and periodically re-configured in accordance with the results of the measurements transmitted by the AP 30, and the MT 50. The operation database 100 stores information concerning the known frequencies used by the operating interfering device 118, measurement parameters to be transmitted to the AP 30 and to the MT 50 to be used as controlling values for the performance of the measurement process. The parameters include but are

not limited to the type of measurement to be made, signal thresholds to be detected, frequencies to check, sub-sets of potentially usable channels, sub-sets of preferred channels, sub-sets of channels used by specific WLANs, geo-locations of specific WLANs with associated RF network topology including sector information, and the like. The operation database 100 is periodically updated by the AP device 30, and/or the MT 50 device with information associated with the detected interference, such as frequencies, interfering signal level, interference periods, error rates, and the like. Interference measurement control 94 is a process designed to manage the interference detection and avoidance functions of the AP device 30 and the MT device 50. The control 94 operates in the application layer level of the HiperLAN/2 protocol. The control 94 is responsible for the overall operation of the DFSNC 92 by coordinating the various functions included therein with the interference detection and avoidance functions implemented in a set of mobile terminal devices. The control 94 operates according to the operating parameters stored within the operation database 100. The control 94 obtains the sub-sets of potentially usable channels from the operation database 100 and communicates the information to the APs. The information may be periodically updated according to channel measurement results and/or the operator's input. The control 94 obtains the measurement parameters from operation database 100 and sends the parameters in association with suitable instruction measurement initiating instructions to the AP device 30 and/or the MT device 50. The interference measurement analysis function 96 is operative in receiving the uploaded result values of the measurements from the AP device 30 and/or the MT device 50, in analyzing the result values, in identifying the presence or absence of an interfering signal on the measured channel and in returning the results produced to the interference measurement control 94. The interference measurement control 94 activates the messaging function 98. The messaging function 98 is responsible for the downloading of the appropriate instructions to the AP device 30 and/or the MT device 50 concerning the initiation of the appropriate interference avoidance actions, such as moving to another channel.

The interference avoidance function 98 sends frequency selection parameters attached to the channel changing instruction, power levels required to the adjustment of transmitted signal levels, and the like. The parameters could also include a range of unusable frequencies, a range of preferred frequencies, RF topology information such as AP locations, AP sectors and the directionality thereof, and the like. In accordance with the geographical location of the AP 30 and the associated mobile terminals thereof different measurement-related or frequency change-related parameters can be downloaded to different mobile terminals. For example, if a known radar transmitter is operating in a defined locality of certain WLANs then APs and/or the mobile terminals within the range of the radar transmitter are instructed not to move to the frequencies known to be used by the radar system. Thus, an on-going dynamic interference detection process is taking place through which the interference-related information in the operation database 100 of the DFSNC is dynamically maintained. The operation database 100 includes but is not limited to a channel parameters changes table, a predefined channel information table, an RF topology information table including APs locations, APs sectors with associated directionality data, a time window control table, and a channel periodicity table. The functionality of the additional tables will be described hereunder in association with the following drawings. Note should be taken that in other embodiments of the present invention other alternative processes, functions, and components could be used, the functionality of the processes can be different, and the operation database and the tables stored therein could be implemented and structured in a number of alternative ways. For example, the user interface unit 101 can be enhanced such as to be utilized in addition to the interactive control of the parameters, for the submission of queries, for producing statistical listings, and the like.

Still referring to Fig. 5 AP 30 includes but not limited to an interference measurement function 102, an interference reporting function 104, an interference avoidance function 106, a messaging function 107, and an operation database 108. The operation database 108 stores diverse measurement

information, channel information, interference information, operating parameters, channel periodicity data, time slot control data, and the like. The operation database 108 enables the AP device 30 to operate independently of the DFSNC 92 under specific circumstances such as in the case of a communication failure between the AP 30 and the DFSNC 92. The table 108 also enables the AP 30 to operate autonomously as defined by the in the different operation modes of the method and system offered by the invention. Thus, following the performance of the required measurements the AP device 30 updates the operation database 108 with the results of the measurement before/after/while sending in the link the information to the DFSNC 92. The interference avoidance function 106 is implemented for activating appropriate interference avoidance options according to the relevant parameters received from the DFSNC 92. The interference measurements function 102 is implemented in the application layer of the protocol stack and is responsible for the activation of the interference detection functions in accordance with the instructions received from the DFSNC 92. The interference reporting function 104 is operative in the sending in the link the results of the measurements to the DFSNC 92. The AP 30 can also instruct the MT 50 to perform the requested interference detection and avoidance operation by sending the necessary parameters to the MT 50. Note should be taken that in other embodiments of the present invention other alternative processes, functions, and components could be used, the functionality of the processes can be different, and the operation database could be implemented in a number of alternative ways.

Still referring to Fig. 5 the MT device 50 consists of but not limited to an interference measurement function 110, an interference reporting function 112, an interference avoidance function 114, a messaging function 117, and an operation database 116. The operation database 116 stores diverse measurement information, channel information, interference information, operating parameters, channel periodicity data, time window control data, and the like. The operation database 112 enables the MT 50 to operate independently of the AP 30, and the DFSNC 92 under specific circumstances such as in the case of a communication

failure along the uplink communication path. The database 116 also enables MT 50 to operate autonomously as defined by the different operation modes of the method and system offered by the invention. Thus, following the performance of the required measurements the MT 50 updates the operation database 116 with the results of the measurements before sending the information to the AP 30. The interference measurements function 110 is implemented in the application layer of the protocol stack and is responsible for the activation of the interference detection functions in accordance with the instructions received from the AP 30. The interference reporting function 112 operative in the sending of the results of the measurements to the AP 30. Note should be taken that in other embodiments of the present invention other alternative processes, functions, and components could be used, the functionality of the processes can be different, and the operation database could be implemented in a number of alternative ways. The substantially modular configuration of the proposed system allows for several varied implementation schemes. Thus, in other embodiments of the invention some or all of the functions implemented in the AP and/or the MT could be implemented in the DFSNC only. Accordingly, a method of interoperability between the mobile terminals of any manufacturer and the DFSNC can be provided. This option enables operators of the WLANs to use third party wireless interference detection solutions from companies that specialize in that area, rather than develop similar solutions in-house.

Still referring to Fig. 5 the AP 30 allocates the channels for operation to the MT 50 according to the instructions received from the DFSNC 92. The AP 30 selects a specific channel for operation by utilizing a list of channels sent by the DFSNC 92. The list contains a sub-set of potentially usable channels and a sub-set of unusable channels. The list could further provide preference information associated with the entries constituting the usable channels sub-set. The AP 30 examines the list, ignores the channels in the unusable channel sub-set and selects a channel from the usable channel sub-set. If preference data is

provided with the usable channel sub-set then the selection could be made in accordance with the preference data.

Fig. 6 illustrates the structure of the operation database implemented on the DFSNC devices, the AP devices, and the MT devices. In different operation modes the structure of the operation database implemented on the different platforms could substantially differ. The operation database 400 includes but not limited to an operating parameters table 402, a measurement parameters table 404, an interference data table 406, a channel data table 408, a channel parameter changes data table 410, a time window data table 412, a network topology table 413, and a channel priority data table 414. The operating parameters table 402 is used for defining the overall interference detection scheme for the interference detection function. The table 402 includes but not limited to lists of installed DFSNCs, APs, MTs, detection process time tables, and the like. The measurement parameters table 404 is utilized by the interference detection mechanism to identify a radar signal. The table 404 includes but is not limited to radar signal characteristics as determined by known radar transmitters, such as frequency, scan rate, pulse width, pulse rise/fall time, power, minimum detectable signal, pulse repetition frequency, pulse recurrence time, pulse duration, and the like. The interference data table 406 includes detected interference values, such as received signal strength, and the like. The data in table 406 is utilized as input to the interference measurement analysis and to channel sub-set allocations. The channel data table 408 includes a list or range of blocked frequencies, a list or range of available frequencies, and the like. The entries in the list or range of frequencies could include preference order and operating conditions, such as date or time of the day. The information stored in the channel data table 406 is used as parameters associated with the interference avoidance instructions sent to the relevant devices. The channel parameter changes table 410 stores lists of changes detected in the channel parameters during the pattern-based detection mode. The time slot data table 412 stores

interfering signal periodicity data. The network topology table 413 includes but not limited to specific network information and device information, such as network identification, device identification, and the like. Table 413 could also include data about the geographical location of the various devices, such as APs, implemented in the network, sector information associated with sectorized devices, such as number of sectors, sector direction, and the like. Table 413 could further include topology information concerning other WLANs in the environment as well as information concerning known, estimated, or identified primary users operating in the vicinity. The primary user information could include known or estimated geographical location, user type, and the like. Table 413 is operative in the creation and maintenance of a transmission/reception coverage map of one or more WLANs. Note should be taken than in other embodiments of the present invention additional tables could be used, such as a historical data table, statistical data table, operators profile table, and the like.

Referring now to FIG. 7 showing an exemplary sequence of functional steps operative in the performance of the interference detection and avoidance process according to the first preferred embodiment of the present invention. The first embodiment implements the DFSNC control mode. At step 119 the operation database implemented on the DFSNC device is updated by the operator of the DFDSNC. The operator is provided with the option of manipulating the parameters of the system in order to enable activation of the interference detection process at certain points in time for the entire set or a limited sub-set of one or more DFSNC devices. The operator of the DFSNC is provided with the capability of inserting, updating and deleting data stored in the operation databases. The data includes but not limited to the set of MT/AP devices to be controlled by one or more DFSNC devices, the set of MT/AP devices required to perform interference detection, a range of frequencies to examine for the presence of interference, a range of frequencies to be used for the re-assignment of the channels being interfered with, or conditionally reassigned, and a range of frequencies blocked or

conditionally blocked for re-assignment or for use. The conditional reassignment or the blocking of the channels can be done in accordance with specific parameter values, such as the date, the time of day, and the like. The operator can further manipulate and modify specific measurement values, such as the examined interference signal threshold levels, and the like. The operator is provided with the option of disabling the interference detection process, of querying the status of the system, of producing varied statistical listings, to change the topology map of the WLAN and/or other neighboring WLANs and/or known/estimated primary users, and the like. Additionally the operator can select the appropriate operation mode of the system, such as the DFSNC control mode, the wireless device control mode, the standard interference measurement (i.e., RSS-based) mode, the pattern-recognition-based interference measurement mode, interference avoidance by the frequency re-assignment option, interference avoidance by transmission power level adjustment, by the activation of the co-existence scheme, and the like. The various operational modes of the proposed method will be described hereunder in association with the respective preferred embodiments of present invention and the accompanying drawings. At step 120 the DFSNC retrieves the necessary parameters from the operation database and at step 122 the DFSNC instructs the specified devices to perform interference detection. The appropriate parameters are sent to the specified devices in association with the instructions. At step 124 a wireless device, such as an AP device and/or an MT device receives the instruction with the accompanying parameter values and at step 126 the AP device and/or the MT device perform interference measurement of a desired specific channel in the specifically defined operation mode in accordance with the measurement parameters received from the DFSNC. The wireless device collects the measurement results, updates the local operation database with the results and at step 128 sends the results to the DFSNC. At step 130 the DFSNC receives the measurement results, analyses the results, updates the operation database, and determines the interference-related status of the examined channel. If the channel measured is recognized such as to include an interfering signal at step 132 the

DFSNC instructs the wireless devices in regard to necessary interference avoidance actions, such as moving to a different channel in the allocated frequency band in order avoid collision between the WLAN channel traffic and the interfering signal therein, to properly adjust transmission power levels in order not to interfere with the transmission/reception of the primary user, or activating the co-existence scheme. At step 134 the wireless device takes the requested avoidance measure updates the local operation database, and notifies the DFSNC by uploading the updates performed.

The proposed method and system provide several operational modes. The different operational modes could be implemented in alternative combinations, and in varied ways, such as being predetermined and pre-set at system generation, or could be dynamically modified by the DFSNC operator at certain points in time according to the circumstances, such as the changing of network topology, the addition, the removal, or the replacement of specific devices, the installation or upgrading of interference detection and avoidance-related functions, new information received concerning a wireless communications system, such as a WLAN, or a primary user, such as a radar system, operating in the vicinity, and the like. A specific operation mode can be uniformly applied across the entire WLAN or several different operation modes could be variably applied to one or more DFSNC devices and associated APs/MTs according to the type of installed devices, the type of functions implemented therein, and the like.

The remote interference detection and avoidance method and system offered by the present invention makes available to the operators of the DFSNCs with the option of dynamic geographical frequency planning. The system and method allows for allocating differential frequency ranges to one or more sets of one or more wireless devices. The allocation can be done dynamically by the network controller according to measurements and feedback received from the devices. The feedback and the measurements results could be used for the building of frequency usage maps, for studies of interference, and for the

diagnostics processes utilized to improve spectrum usage. The method and system advantageously allows the WLAN operators to outsource the interference detection and prevention functions to third party developers having suitable expertise in the specific field and having the capability to centrally implement required modifications, changing basic DFS data, such as information concerning new radar installations, satellite feeder transmitters, recent DFS algorithms, and the like. Outsourcing the process to expert third parties can benefit the entire industry and the regulating bodies by enabling the regulators to inspect and control a substantially limited number of interference detection and avoidance packages rather than obliging each individual WLAN manufacturer to go through extensive testing procedures in order to receive authorization for the utilization of their own interference detection and avoidance systems.

Referring now to Fig. 8 showing an exemplary sequence of functional steps operative in the performance of the interference detection and avoidance process, in accordance with a second preferred embodiment of the present invention. The second preferred embodiment of the present invention implements the wireless device control mode. A set of one or more relevant wireless devices includes a modified version of the DFSNC control functions. A higher-level operation database and a set of specific higher-level operation database-related supporting functions are implemented in the DFSNC. At step 500 the higher-level operation database implemented on the DFSNC is updated by the operator of the DFSNC. The operator is provided with the capability of modifying the parameters of the system to enable activation of the interference detection process at certain points in time for the entire set or a sub-set of one or more wireless devices. The operator can also insert into the operation database parameters, such as a set of one or more of MTs/APs desired to perform interference detection, a range of frequencies to examine, a range of frequencies to be used for the re-assignment of the channels being interfered with, and a range of frequencies blocked for re-assignment or for use. The operator can further manipulate and modify specific

measurement values, such as the examined interference signal threshold level, and the like. The operator is provided with the option of disabling the interference detection process, of querying the status of the system, of producing varied statistical listings, to change the topology map of the WLAN, of the primary users, and the like. At step 502 the parameters from the higher-level operation database of the DFSNC are downloaded to the wireless devices according the instructions of the DFSNC operator. In the wireless device control mode the control of the interference detection and avoidance process is made autonomously by the wireless devices. The process loop describing the operation of the wireless device is described across step 504 through step 516. At step 504 the local interference detection control function implemented in the wireless device retrieves the necessary parameters from the local operation database and at step 506 the local control function initiates the performance of the interference detection process. The appropriate parameters are obtained from the local operation database. At step 508 the wireless device, such as an AP and/or a MT perform interference measurement of the specific channel in the specific operation mode in accordance with the measurement parameters received from the local operation database. The wireless device collects the measurement results, updates the local operation database with the results, at step 510 analyses the results, and determines the interference-related status of the examined channel. If the channel measured is recognized such as to include an interfering signal the wireless field performs the consequent interference avoidance actions, such as clearing the measured channel and moving to a different channel in order avoid collision between the WLAN channel traffic and the interfering signal therein. At step 512 the wireless device performs interference avoidance measures. At step 514 the local operation database of the wireless device are updated and at step 516 the device sends the results of the interference detection and interference avoidance process to the DFSNC in order to update the operation database established therein. Process control then proceeds to step 504 to resume the interference detection loop.

The method according to the second preferred embodiment allows the operators of wireless networks the option of controlling the network adaptively. The operators receive dynamic up-to-date information from the devices concerning primary user-related interference, which was detected by the devices. According to the received information the operators can adaptively control the network, such as manually introduce information concerning known primary users and sending the updated information to the devices.

In the pattern-recognition-based interference detection mode interfering sources in the range of a WLAN transmitting radio signals on the same frequency used by a WLAN channel can be detected without the need to be aware of the identity, and characteristics of the transmitter in order to detect the signals interfering with the signals of the WLAN. The method proposed in the pattern-recognition-based mode is based on the identification of one or more specific patterns discernible in a set of changes occurring on the time axis in the parameters of a measured WLAN channel. The measurement is performed as part of the normal operation of the wireless device, such as an AP device and/or MT device. In the pattern-recognition based mode the wireless device performs interference detection and avoidance simultaneously with the standard data exchange operations taking place between the various devices of the network. Thus, no specific time slots need to be allocated for the performance of the interference detection process.

In yet another operation mode, the wireless device still performs the ongoing measurements, but the pattern recognition is performed at the DFSNC. The wireless device reports the collected channel-specific measured anomalies, such as identified errors. The wireless device sends the data along with associated parameters, such as timestamps, periods, and the like to the DFSNC device. Subsequently, the DFSNC device itself performs the pattern recognition process.

The patterns that can be identified as part of the normal operation of the wireless device are related to the basic channel parameters, such as the error

rate changes including bit error rates, frame error rates, packet error rates, signal-to-noise (SNR) changes, phase shift differentials, and the like. Patterns in the continuously changing channel parameters can be recognized on the data carriers, on the pilot carriers, and optionally on the control carriers. In the pattern-recognition-based mode the wireless device will record changes in the channel parameters and will attempt to detect a pattern in the changes. The pattern recognition method may utilize thresholding functions, statistical analysis functions to account for small fluctuations in the range of the changes and/or in the range of the period in which the changes occur, or Artificial Intelligence (AI) implementations such as used by commercially available neuron networks. Threshold values can be used for defining the time slots during which the changes are to be repeated to form a meaningful pattern and/or for defining the longest time slot without changes. The interference detection can be performed upon any specific combination of the channel parameter changes.

Referring now to Fig. 9 showing an exemplary sequence of functional steps operative in the performance of the interference detection and avoidance process according to the third preferred embodiment of the present invention. In the third preferred embodiment the system implements the pattern-recognition-based interference detection mode. At step 600 a signal is received by the wireless device. At step 602 the signal is sampled and converted to digital format by an analog-digital converter. At step 604 the pattern analysis parameters are read from the operation database. At 606 the pattern analysis is performed by obtaining the suitable channel parameters, such as error rates, SNR changes, and the like, building channel parameters changes lists and processing the lists by appropriate analysis functions, such as the Histerhasys function, the neuron network, or the like. At step 608 an interference pattern is recognized on the examined channel, and appropriate interference avoidance actions are performed, such as moving to a vacant channel within the allocated frequency

band. At step 610 the operation database are updated with the relevant data, and at step 612 the updates are optionally uploaded to an AP and/or the DFSNC.

Note should be taken that in another operational mode the steps 606 through 610 could be performed in the DFSNC device and step 612 could be replaced by a reporting step to the wireless device.

The pattern-recognition-based interference detection mode proposed by the method and system of the present invention is performed on an on-going basis rather than in "interrupted" periods, which may or may not include the interfering signals. The performance of interference detection in this mode requires neither information in respect to the radar systems operating within the range of the WLAN nor decisions by the higher layers of the communications protocol or the remote network controller. Yet the method could be combined with and be assisted by radar system-related information and/or by certain decisions made in the higher layers of the communication protocol. For example, if certain radar systems are known to have a fixed 10 seconds "sweep" rotation period then the wireless devices channel measurements functions could be calibrated such as to perform the channel measurements having the same 10 seconds periodicity. The operational decisions concerning the presence and/or the power level of interference and can be made locally by the low layers of the wireless device based on the locally accumulated and locally analyzed channel parameter information. In addition the information is collected without interrupting the on-going standard data exchange operations of the network.

Note should be taken that in other operational mode the decisions could be made in the DFSNC. Thus, the WLAN operators will be provided with the option to outsource the interference detection and prevention process to a third party.

The co-existence mode relates to the adaptive modification of a WLANs transmission parameters in response to the detection of a periodic interference detected by one of the interference detection schemes described

above, or known in advance. Many of the radar systems transmit periodically. Therefore WLAN devices operating in the vicinity of a periodic radar systems will be periodically effected by the interference caused by the signals emitted from a radar system transmitting on the frequency utilized by a WLAN device, and similarly periodically effect the same radar by the WLAN signals. In current wireless system when a periodic interference detected the channel used by a wireless device is re-assigned to a different channel. The detection of a periodic interference will cause activation of a process in the WLAN that will provide the capability for both systems operating in the same geographical area within broadcast range to keep functioning effectively on the same channel. Thus, a substantially improved utilization of the allocated bandwidth is achieved, which is specifically important in the about 5 GHz spectrum including periodic transmitters, such as pulse/sweep radar systems. Co-existence on the same channel allows better utilization of the allocated spectrum while not compromising the operation of the primary user, such as a radar system. The resulting negative impact on the performance of the wireless communications system, such as a WLAN, is non-existent or negligible.

Fig. 10 illustrates an exemplary sequence of functional steps operative in the performance of the interference detection and avoidance process that implements the co-existence scheme. At step 700 a signal is received by the wireless device of the WLAN. At step 702 the signal is sampled and converted to digital format by an analog-digital converter. At step 704 interference periodicity measurements are performed by the wireless device of the WLAN. At step 706 the interference periodicity measurement results are collected into suitable lists and at step 706 the lists are processed and analyzed in an attempt to recognize systematic periodicity of the interference. At step 708 the systematic periodicity of the interference is established and an appropriate time slot table is set up. In the time slot table the wireless device of the WLAN allocates vacant time slots to its WLAN devices such that the interfering primary user will continue to operate

uninterrupted and the interfered WLAN will keep functioning without interrupting the interfering primary user. Within the allocated time slot stored in the time slot table the entire wireless network associated with the WLAN will be instructed not to transmit or alternatively to adjust its transmission power such as not to interfere with the periodically transmitting primary user, such as a pulse radar. As a result within the allocated time slots the WLAN will not interfere with the signals transmitted by the primary user either by not transmitting or by lowering the power levels of the signals transmitted. At step 710 the time slot table and related information from the operation database uploaded to a network controller for appropriate processing. At step 712 the network controller analyzes the uploaded time information and performs a suitable co-existence related process. The process is designed to allow both the wireless network and the primary user to continue operating on the same channel on a specific frequency by instructing the wireless network not to transmit during the time slots allocated to the signal of the primary user.

Note should be taken that the periodicity measurements, the analysis of the results, and the building of the time window table could be performed in diverse other manners. For example, the appropriate periodicity data could be received from the operators of a known primary user operator and could be inserted into the suitable table by the wireless network operator or the DFSNC operator. Similarly the process of analysis, and the time window table maintenance could be initiated by the wireless network operator or the DFSNC operator. The relevant tables could be then stored on the controller device and could be controllably downloaded when necessary to the wireless device.

Fig. 11 illustrates graphically a signal collision and an exemplary solution thereof in a WLAN channel. Signal 801 is a WLAN signal comprising MAC frames 800, 802, 804, 806, 808 transmitted via a link set up between two or more WLAN devices such as an AP and a MT on an assigned WLAN channel having a specific frequency allocated thereto. Signal 803 is a continuous radar

signal transmitted via air interface by a radar transmitter. Signal 801 and signal 803 are transmitted on the same frequency. The receiving WLAN wireless device, such as a MT device, is deployed such that the device is in the operative range of the radar transmitter emitting signal 803. As a result the WLAN wireless device, such as a MT device, is receiving simultaneously both signals 801 and 803. The signal 801 is overlaid in the specific communication channel associated with the MT device by signal 803 and the resulting signal 805 is a corrupted version of signal 801. The signal 805 is referred to as interference where the interference is created by the unintended reception of signal 802. Similarly, the reception of the WLAN signal 801 by the primary user effects interference to the same primary user. In the preferred embodiment of the present invention the signal 805 is detected by the interference detection method and system described hereinabove. Consequent to the detection of the corrupted signal 805 specific interference avoidance functions are activated and a number of alternative interference countermeasure actions are taken. One such action includes interference avoidance, such as changing the communication path of the signal 801. After a suitable time interval 801 required for the performance of the channel switching operation, the path is changed by switching from channel 807 to a new channel 809 transmitted on an unused frequency 809. The WLAN signal 801 comprising the MAC frames 800, 802, 804, 806, and 806 will be transmitted undisturbed on the newly allocated channel 809 while the radar signal will keep transmitting on the original channel 805.

Fig. 12 illustrates graphically a signal collision and an alternative solution thereof in a WLAN channel according to the preferred embodiment of the present invention. Signal 811 is a WLAN signal comprising MAC frames 800, 802, 804, 806, 808. Signal 811 is transmitted via a link set up between two or more WLAN devices such as an AP and a MT on an assigned WLAN channel having a specific allocated frequency. Signal 814, 816, 818 are a set of periodic radar signal transmitted via air interface by a radar transmitter for radio-location

and ranging purposes. Signal 811 and signals 814, 816, 818 are transmitted on the same frequency. The receiving WLAN wireless device, such as a MT, is deployed such that the device is in the operative range of the radar transmitter emitting periodic signals 814, 816, 818. As a result, the WLAN wireless device, such as a MT device, is receiving simultaneously both signals 811 and periodic signals 814, 816, 818. The signal 811 is overlaid in the specific communication channel associated with the MT device by the periodic signals 814, 816, 818 and the resulting signal 813 is a corrupted version of signal 811. The signal 813 includes periods of interference 812', 812'', and 812'''. that correspond to the reception of the interfering periodic signals 814, 816, 818. Signal 815 represent the WLAN signal train as transmitted in the channel subsequent to the activation and completion of the co-existence option if no channel switch was performed by the WLAN after the detection of the primary user as stated in the other embodiments. Signal 815 comprises intermittent WLAN traffic consisting of MAC frames 822, 826, 830, time guard intervals 823, 823', 823'', 823''', 823'''', and periodic "WLAN silence" time slots 824, 828, and 832. The periodic WLAN silence slots correspond to the duration of the periodic radar signals 814, 816, 818 that were detected, analyzed and collated by the appropriate interference detection functions. In order to enable co-existence with the radar, and to allow undisturbed transmission of the periodic radar signals, for the duration of time slots 824, 826, 828 the transmission of signals between the entire set of WLAN devices is suspended or powered down. The WLAN silence slots 824, 826, 828 are suitably separated by configurable time guard intervals 823, 823', 823'', 823''', and 823''''.

Implementing the co-existence mode provides the operators of a WLAN with the option of spreading out the network across a wide frequency range. Thereby the overall useable bandwidth capacity of the network is increased and a significant improvement is achieved in the utilization of the unlicensed 5 GHz spectrum. The present invention provides operators of a WLAN and the spectrum regulators a mechanism to ensure compliance with the regulations and

with the changing deployments of primary users, such as radar systems, satellites, amateur radio service, and the like. The remote mechanism as offered by the preferred embodiments of the present invention provides the capability to co-exist even on frequencies certain primary users are known to operate thereon.

In wireless network containing on or more sectorized wireless devices basic sector-related information can be provided to the controller device (DFSNC) by multiple network operators. The sector information, such as the list of sectorized devices, the number of sectors included within each device, the directionality of the specific sector, and the like, will be stored within the operation database established on the controller device (DFSNC). The interference detection data communicated by a sectorized wireless device will include information concerning the specific sectors on which the interfering signals were detected. As a result, the controller device will have substantially precise information in respect to the location of the interfering primary user device and/or neighboring WLANs. The location of the devices could be communicated to other wireless networks operating in the same environment but located at a distance further from the interfering source and therefore less likely to detect it. Thus, the controller device can be used as an assessor for the other wireless networks based on the information collected by other wireless networks.

Additionally the interference avoidance measures taken by the wireless devices could be sector specific. For example, when on sector X an interfering source is detected the controller could instruct the reporting wireless device to cease periodically or permanently transmitting only on sector X, or adjust the signal power levels only on sector X while continue normal operations on the other sectors.

Referring now to Fig. 13 illustrating the operation the method and system in accordance with the fourth preferred embodiment of the present invention. The operation described involves a detector AP implemented in association with one or more WLANs having a sectorized or an omnidirectional

mode of operation. The detector AP can operate either in an omnidirectional mode or in a sectorized mode. A sectorized detector AP is used to provide additional information in regard to the directionality of the detected signals. A sectorized detector AP 812 is co-located with a primary user, such as a radar system 802. A sectorized AP 804, a sectorized AP 816, and an omnidirectional AP 808 operate in the environment within various transmission/reception coverage areas and transmission/reception ranges from the radar system 802. The sectorized AP 804 includes a transmission/reception coverage sector 830, a sector 832, a sector 834, a sector 836, a sector 838, and a sector 840. For purposes of readability the sectors included in the sectorized AP 822 are not shown. Each AP 804, 806, 808 has the capability of controlling several MTs. The drawing illustrates that the AP 804 controls a MT 818, a MT 820, the AP 806 controls a MT 814, a MT 822, and the AP 808 controls a MT 824. Although only a limited number of APs and MTs are shown it will be readily understood that in a realistic environment several APs could be implemented controlling several MTs. Note should be taken that the different APs could be associated with different WLANs.

The transmission/reception coverage area of each of the six sectors included in AP 804 is covering an azimuth of about 60 degrees. Lines 854, 856 indicate the limits of the transmission/reception coverage area of the sector 832. When the WLAN AP 804 transmits through the sector 832 the signals may interfere with the radar system 802. When the AP 804 transmits through the other sectors 830, 834, 836, 838, 840 no interference is effected with the radar 802 due to the differential directionality of the transmission. In contrast when the radar 802 is transmitting, the radar signals may interfere with the section 832, and with the section 838, which is within the transmission/reception directional reception line of the radar 802.

The detector AP 812 receives the transmission of the APs 804, 806, 808 via link 850, 846, 852 respectively. Link 850, 846, 852 could be a wireless link or a wired link. In accordance with the diverse transmission/reception ranges between the detector AP 812 and the APs 804, 806, 808 the respective power

levels of the signals received by the detector AP 812 could be different in respect to each of the APs. Under certain circumstances, for example when the APs are deployed such that the detector AP 812 is out of their effective broadcast range, the detector AP 812 may not detect the signals transmitted by specific APs.

A DFSNC 810 is coupled to the WLAN APs 808, 806, 804 via links 840, 842, and 844 respectively, for purposes of communication and control. The DFSNC 810 could be co-located within one the WLAN APs or could be deployed on an independent platform within one of the WLANs. The detector AP 812 is normally instructed to be functionally receptive to signals transmitted on the channel used by the radar system 802. Thus, the detector AP 812 also has the capability of detecting the radar system's transmission periods directed towards each transmission/reception coverage sector associated with the WLAN devices. The detector AP 812 is utilized to detect the "sweep" of the radar or the temporal and directional position of the radar's radiation pattern during the full rotational period of the radar's antenna. The detector AP 812 is also responsible for detecting the transmission of different WLANs operating in the vicinity of the radar system 802 by identifying the radiating sources. Those sources can be APs and the associated MTs thereof implemented across different WLANs operating in the vicinity of the radar system 802. If the detector AP 812 is non-sectorized then the information acquired will have no directional dimension. In contrast, if the detector AP 812 is sectorized then the reception information will have directional dimension. Thus, at a certain point in time the sectorized AP 812 will receive on one of the sectors thereof the radar signal as a part of the radar "sweep" while on the rest of the sectors thereof various WLAN signals will be received. The detector AP 812 is further provided with the capability of detecting various MTs operating in the WLANs that are deployed near the radar system 802. Thus the detector AP 812 acquires further indication of the fact that a WLAN operates on the radar system's 802 channel. Subsequently the detector AP 812 notifies the DFSNC 810 through the link 846 concerning the collected results of the signal detection process performed in the environment.

In a similar manner, the APs 804, 806, 808 sends the results of the interference detection measurements performed thereby to the DFSNC 810 via the links 844, 842, 840. If the APs are sectorized then the uploaded information includes directional dimension. The information received from detector AP 812, AP 804, AP 806, and AP 808 is analyzed by the DFSNC 810 and in combination with the data the DFSNC 810 already has in respect to the location of the various APs, and the directionality of their respective sectors, the channels utilized, the location and parameters of the radar, and other relevant data. The result of the analysis enables the DFSNC 810 to build up a RF topology mapping of the signal environment. In accordance with the "signal environment map" the DFSNC 810 performs specific predefined measures in order to co-ordinate the signaling activities of the diverse wireless devices. For example, in order to accomplish signal harmony in the environment the DFSNC 810 could notify the AP 804, and the AP 806 to cease transmission for specific periods of time following the detector AP 812 notification in regard to the radar system 802 "sweeping" movement in time and space. Utilizing the directional information the DFSNC 810 has concerning the AP 804, and the AP 806, the DFSNC 810 could further specify that only specific sectors need to be "silent", such as sector 832 and sector 836 in AP 804, while the rest of the sectors, such as sector 834, 836, 830 may continue normal or powered down operations. Additionally, due to the dynamic time allocation process within the MAC frame, some APs, such as AP 804 could utilize the time allocated originally for the sector 832 and sector 836 such as to be used by the other sectors, such as sector 843, 836, and 830. As a result the AP over-all time-related capacity is preserved.

The extensive signal environment map data established by DFSNC 810 enables DFSNC 810 to control WLAN devices that are unable to detect interference independently due to their distance from the interfering transmission source. For example, the currently discussed drawing shows AP 808 deployed such that it is more remote from the radar system 812 than the AP 804, and the AP 806. Thus, AP 808 may not be able to detect interfering radar signals emitted

by radar system since the signals received will be having a power level lower than the signal detection threshold provided to the interference measurement mechanism of AP 808. Yet at the same time the transmission of AP 808 may interfere with the radar system 802 due, for example to the higher sensitivity of the radar's receiver. Utilizing the signal environment map the DFSNC 810 can notify the AP 808 to take specific interference avoidance measures, such as to cease transmitting, or to lower the transmission power thereof.

The detector AP 812 co-located with the primary user, such as the radar system 802 can be utilized for detecting the signals transmitted by other WLANs as received at the site of the primary user. Subsequently the detector AP 812 notifies the DFSNC 810 AP-specific information, such as AP identification, network identification, received signal strength (RSS) and the like. If the transmitting AP operates in a sectorized mode then the detector AP 812 sends to the DFSNC 810 the appropriate directional information. The directional information enables the DFSNC 810 to instruct the suitable device, such as the AP, to take predefined interference avoidance measures, such as ceasing transmission, or lowering transmission power on one or more of its existing sectors.

The detector AP 812 co-located with the primary user, such as the radar system 802 is also operative in tracing the primary user, such as radar system 802 "sweeping" movement. Subsequently the detector AP 812 can notify the DFSNC 810 in regard to the temporality and directionality of the "sweep" process. The communicated and analyzed information provides the DFSNC 810 with the capability to instruct the WLANs deployed on the path of the radar antenna's sweep to take predefined interference avoidance measures, such as interrupting transmission or lowering transmission level on one or more existing sectors.

It will be easily perceived by one with ordinary skill in the art that the steps and components mentioned in the foregoing description were provided as examples and were not intended to be limiting. Diverse other components and

methods could be used to accomplish the underlying objectives of the present invention and several enhancements and improvements to the described embodiment could be contemplated within the framework of the general issues inherent in the proposed system.

The above description of the construction and use of systems incorporating a plurality of mobile terminals, access points, network controllers, transceivers, and the like makes particular reference to use in a land-based wireless local area network (WLAN). However, it will be understood that the use of the technique is in no way limited to land-based wireless local area networks and that it is equally applicable to wireless wide area networks, and other fixed and/or mobile wireless communication systems incorporating satellite links.

Persons skilled in the art will appreciate that the present invention is not limited to what has been particularly shown and described hereinabove. Rather the scope of the present invention is defined only by the claims, which follow.

I CLAIM:

1. In a wireless communications environment accommodating at least one secondary user transmitting and receiving a radio frequency signal on an allocated frequency band via an air interface, at least one primary user transmitting and receiving a radio frequency signal on a substantially alike allocated frequency band via an air interface, a method for the detecting and avoiding reciprocal signal interference produced by the radio frequency signals emitted by the at least one primary user and by the at least one secondary user, the method comprising the steps of:

   establishing dynamic interference detection and avoidance control and operation information in the at least one secondary user; and

   dynamically and controllably measuring at least one communication channel providing a communication path between at least two wireless devices of the at least one secondary user; and

   analyzing the results of measurements performed on the at least one communications channel in order to determine the interference status of the measured at least one communications channel of the at least one secondary user; and

   dynamically maintaining interference detection and avoidance information in the at least one secondary user; and

   selectively performing controllable interference avoidance procedures by the at least one secondary user to prevent reciprocal signal interference in the at least one secondary user and in the at least one primary user.

2. The method of claim 1 further comprising selectably performing a signal co-existence procedure to enable co-existence of the at least one secondary user with the at least one primary user on the substantially alike pre-allocated frequency band in the communications environment.

3. The method of claim 1, further comprising the at least one secondary user communicating interference detection and avoidance information and instructions to at least one other secondary user.

4. The method of claim 1 wherein the step of establishing comprises the steps of:

maintaining communications environment status information in the at least one secondary user; and

creating detected signals information in the at least one secondary user; and

building interference measurement information in the at least secondary user; and

originating interference avoidance information in the at least one secondary user.

5. The method of claim 1, wherein the step of measuring comprises the steps of:

sending interference measurement control information to at least one interference detection and avoidance wireless device by the interference detection and avoidance controller device of the at least one secondary user; and

instructing the at least one interference detection and avoidance wireless device to perform interference measurements with respect to at least one communications channel by the interference detection and avoidance controller device of the at least one secondary user; and

performing interference measurements by the at least one interference detection and avoidance wireless device on the at least one communications channel; and

communicating the results of the interference measurements by the at least one interference detection and avoidance wireless device to the interference detection and avoidance controller of the at least one secondary user.

6. The method of claim 1, wherein the step of measuring comprises the steps of:

examining the parameters of the signal received on the at least one measured communications channel by the at least one interference detection and avoidance wireless device; and

comparing the received signal parameters with the suitable interference detection information communicated by the interference detection and avoidance controller.

7. The method of claim 1, wherein the step of performing comprises the steps of:

modifying the suitable interference avoidance procedure by the interference detection and avoidance controller; and

selecting the suitable interference avoidance procedure by the interference detection and avoidance controller; and

communicating the suitable interference avoidance procedure and attached interference avoidance information to the at least one interference detection and avoidance wireless device by the interference detection and avoidance controller; and

executing the communicated interference avoidance procedure by the at least one interference detection and avoidance wireless device.

8. The method of claim 5, wherein the step of interference measurements performance is executed by the at least one interference detection and avoidance controller device.

9. The method of claim 5, wherein the step of interference avoidance performing is executed by the at least one interference detection and avoidance controller device.

10. The method of claim 1, wherein the step of maintaining interference detection and avoidance control and operation information further comprises:

manually maintaining the interference detection and avoidance information stored in the operation database by an operator of the secondary user in accordance with information received from external sources; and

dynamically maintaining the interference detection and avoidance information stored in operation database by interference detection and avoidance device; and

dynamically maintaining the interference detection and avoidance information stored in operation database by interference detection and avoidance service.

11. In a communication environment accommodating at least one secondary user transmitting and receiving a radio frequency signal on a pre-allocated

frequency band via a link, at least one primary user transmitting and receiving a radio frequency signal on a substantially same pre-allocated frequency band via an unbounded medium, a system for the dynamic detection and avoidance of reciprocal signal interference produced substantially simultaneously by the at least one secondary user and at least one primary user, the system comprising the elements of:

at least one primary user interference detection and avoidance controller device; and

at least one primary user interference detection and avoidance wireless device.

12. The system of claim 11, wherein the at least one controller device comprises the elements of:

an interference measurement control function to instruct at least one interference detection and avoidance wireless device to perform interference detection; and

an interference measurement analysis function to identify the type, the quality, and the source of the measured interference; and

an interference avoidance control function to instruct at least one interference detection and avoidance wireless device to perform interference avoidance procedures; and

a messaging function to communicate the instructions to the at least one interference detection and avoidance wireless device; and

a user interface function to enable an operator to create and maintain the operation database; and

an operation database to hold interference detection parameters, interference avoidance parameters, network information, wireless device information, available channel information, channel periodicity data, primary user information, measurement results, and general operating parameters.

13. The system of claim 12, wherein the operation database comprises the elements of:

an operating parameters table utilized to control interference detection modes, interference avoidance methods, secondary user information, primary user information; and

a measurements parameter table to determine the operative parameters of the interference detection process ; and

an interference information table to provide information in regard of the interference detected on the at least one communication table; and

a channel data table to provide usable and non-usable communication channel information; and

a channel parameter changes table to hold the collection of the channel anomalies; and

a time window data table to indicate operational periods of a periodically operative primary user; and

a channel periodicity table to hold a set of consecutive time slot values functional in enabling the at least one secondary user and the at least one primary user to use co-operatively the same communication channel; and

a network topology data table to provide information concerning the at least one secondary user, the at least one secondary user devices, and the at least one primary user.

14. The system of claim 11, wherein the at least one interference detection and avoidance wireless device comprises the elements of:

an interference measurement function to selectively measure at least one communication channel operative in the linking of at least two wireless devices of the at least one secondary user; and

an interference avoidance function to perform interference avoidance measures; and

an interference reporting function to assemble and structure messages concerning the results of the interference measurement functions; and

an operation database to hold interference detection parameters, interference avoidance parameters, network information, wireless device information,

available channel information, channel periodicity data, primary user information, measurement results, and general operating parameters.

15. The system of claim 11, wherein the at least one interference detection and avoidance device wireless device further comprising a messaging function to communicate the results of the interference measurements performed by the wireless device to the interference detection and avoidance controller device.

16. The system of claim 14, wherein the interference avoidance function comprises the elements of:

a channel re-assignment function to avoid mutual interference between the at least one secondary user and the at least one primary user by providing the at least one communicating wireless devices of the secondary user with an alternative communication channel ; and

a transmission power adjustment function to prevent interference to the at least one primary user dynamically lowering the transmission, power level of the signal radiated by the at least one secondary user; and

a co-existence function suitably dividing the communication channel into mutually exclusive time slots providing the at least one secondary user and the at least one primary user to utilize the channel co-operatively and alternately.

17. The system of claim 14, wherein the interference measurement function comprises the elements of:

a received signal strength measurement function; and

a received signal period measurement function to examine the power level of the signal received on the at least one communications channel; and

a channel anomalies measuring function to collect and collate channel anomalies during the routine data exchange operations on the at least one communications channel; and

a received signal periodicity identifier function to describe the transmission periods at least one periodically transmitting primary source.

18. The system of claim 11, wherein the at least one primary user interference detection and avoidance controller device is collocated with the at least one primary user interference detection and avoidance wireless device.

19. The system of claim 14, wherein the at least one secondary user is a wireless local area network (WLAN).

20. The system of claim 19, wherein the WLAN is a HiperLAN/2-type network.

21. The system of claim 19, wherein the WLAN is an IEEE 802.11a-type network.

22. The system of claim 19, wherein the WLAN comprises at least one transmitting and receiving wireless devices.

23. The system of claim 19, wherein the WLAN comprises at least one sectorized wireless devices operative in transmitting and receiving via at least one operative sectors having different radiation directionality.

24. The system of claim 19, wherein the WLAN is coupled to a wired communications network.

25. The system of claim 24, wherein the wired communications network is a local area network (LAN).

26. The system of claim 24, wherein the wired communication network is wide area network (WAN).

27. The system of claim 19, wherein the WLAN is operative in communicating interference related information and instruction to other secondary users.

28. The system of claim 11, wherein the at least one primary user is a radar system.

29. The system of claim 28, wherein the radar system is a continuous wave (CW) radar system.

30. The system of claim 28, wherein the radar system is a pulse/sweep radar system.

31. The system of claim 11, wherein the at least one primary user is a satellite feeder system.

32. The system of claim 11, wherein the at least one primary user is an amateur radio service.

33. In a wireless communications environment accommodating at least one secondary user transmitting and receiving a radio frequency signal on a pre-allocated frequency band via an air interface, at least one primary user transmitting and receiving a radio frequency signal on a substantially alike pre-allocated frequency band via an air interface, a method of detecting and avoiding signal interference effected to the at least one primary user by the transmission of the signal emitted by the at least one secondary user, the method comprising the steps of:

dynamically and controllably measuring at least one communications channel utilized the at least one primary user; and

analyzing the results of the channel measurements performed on the at least one communications channel utilized by the at least one primary user in order to determine the interference status of the measured channel; and

communicating the results of the analysis to the at least one secondary user interference detection and avoidance controller device; and

dynamically maintaining interference detection and avoidance information concerning the identity, attributes, locations, directionality, and activity of at least one wireless device associated with at least one secondary user interfering with the at least one measured communications channel associated with the at least one primary user;

selectively and controllably performing interference avoidance measures by the at least one secondary user interference detection and avoidance controller device to prevent signal interference in the at least one communications channel associated with the at least one primary user.

34. The method of claim 33 further comprising building and maintaining a functional RF topology mapping of the communication environment.

35. The method of claim 33 further comprising selectably and controllably performing a signal co-existence option to enable shared utilization of the at least one communications channel by the at least one primary user and the at least one secondary user.

36. The method of claim 35, wherein the co-existence of the at least one secondary user with the at least one primary user on the substantially alike at least one communications channel is accomplished by selectively adjusting the transmission power level of the signals radiated by the at least one secondary user.

37. The method of claim 35, wherein the co-existence of the at least one secondary user with the at least one primary user on the substantially alike at least one communications channel is accomplished by selectively ceasing transmission of the signals by the at least one secondary user for the duration of the signals transmitted by the at least one primary user.

38. The method of claim 35, wherein the adjustment of the transmission power level performed specifically for at least one directional sector associated with at least one wireless device associated with the at least one secondary user.

39. The method of claim 35, wherein the interruption of the transmission of the signals by the at least one secondary user performed specifically on at least one directional sector associated with at least one wireless device associated with the at least one secondary user.

40. In a communication environment accommodating at least one secondary user transmitting and receiving a radio frequency signal on a allocated frequency band via a link, at least one primary user transmitting and receiving a radio frequency signal on a substantially same allocated frequency band via an unbounded medium, a system for the dynamic detection of reciprocal signal interference produced substantially simultaneously by the at least one secondary user and at least one primary user, the system comprising the elements of:

at least one primary user interference detection and avoidance controller device to communicate with and control at least one secondary user activity detection wireless device; and

at least one secondary user activity detection wireless device to perform measurements on at least one communication channel utilized by the primary user in order to detect interference produced by the activity of at least one secondary user.

41. The system of claim 40, wherein the at least one primary user interference detection and avoidance device is collocated with the at least one primary user.

42. The system of claim 40, wherein the at least one secondary user is a wireless local area network (WLAN).

43. The system of claim 40, wherein the at least one secondary user is a cellular telephone network.

44. The system of claim 40, wherein the at least one secondary user is a Wireless Personal Area Network (WPAN).

45. The system of claim 42, wherein the WLAN comprises at least one transmitting and receiving wireless device.

46. The system of claim 42, wherein at WLAN comprises at least one sectorized wireless device operative in transmitting and receiving in via the at least one sector having specific radiation directionality.

47. The system of claim 40, wherein the at least one primary user is a radar system.

48. The system of claim 43, wherein the radar system comprises a sweep/pulse radar.

49. The method of claim 1, wherein the wireless communications environment accommodates at least two secondary users.

50. The method of claim 1, wherein the method of detecting and avoiding interference is operative in the detection and avoidance of reciprocal signal

interference produced by the radiation of radio frequency signals emitted by the at least two secondary users.

51. The system of claim 11, wherein the communications environment accommodates at least two secondary systems.

52. The system of claim 11, wherein the system for the detection and avoidance of the signal interference is operative in detecting and avoiding signal interference between at least two secondary systems.

53. The method of claim 33, wherein the wireless communications environment accommodates at lest two secondary users.

54. The system of claim 40, wherein the communication environment accommodates at least two secondary users.

55. The system of claim 12, wherein the operation database is implemented on the primary user detection and avoidance wireless device.

56. The system of claim 13, wherein the network topology data table provides information concerning at least two secondary users and at least two secondary users devices.

57. The system of claim 16, wherein the channel re-assignment function is operative in avoiding mutual interference between at least two secondary users.

58. The system of claim 16, wherein the co-existence function is implemented on the interference detection and avoidance controller device.

59. The system of claim 19, wherein the at least one secondary user is a cellular phone network.

60. The system of claim 19, wherein the at least one secondary user is a Wireless Personal Area Network (WPAN).

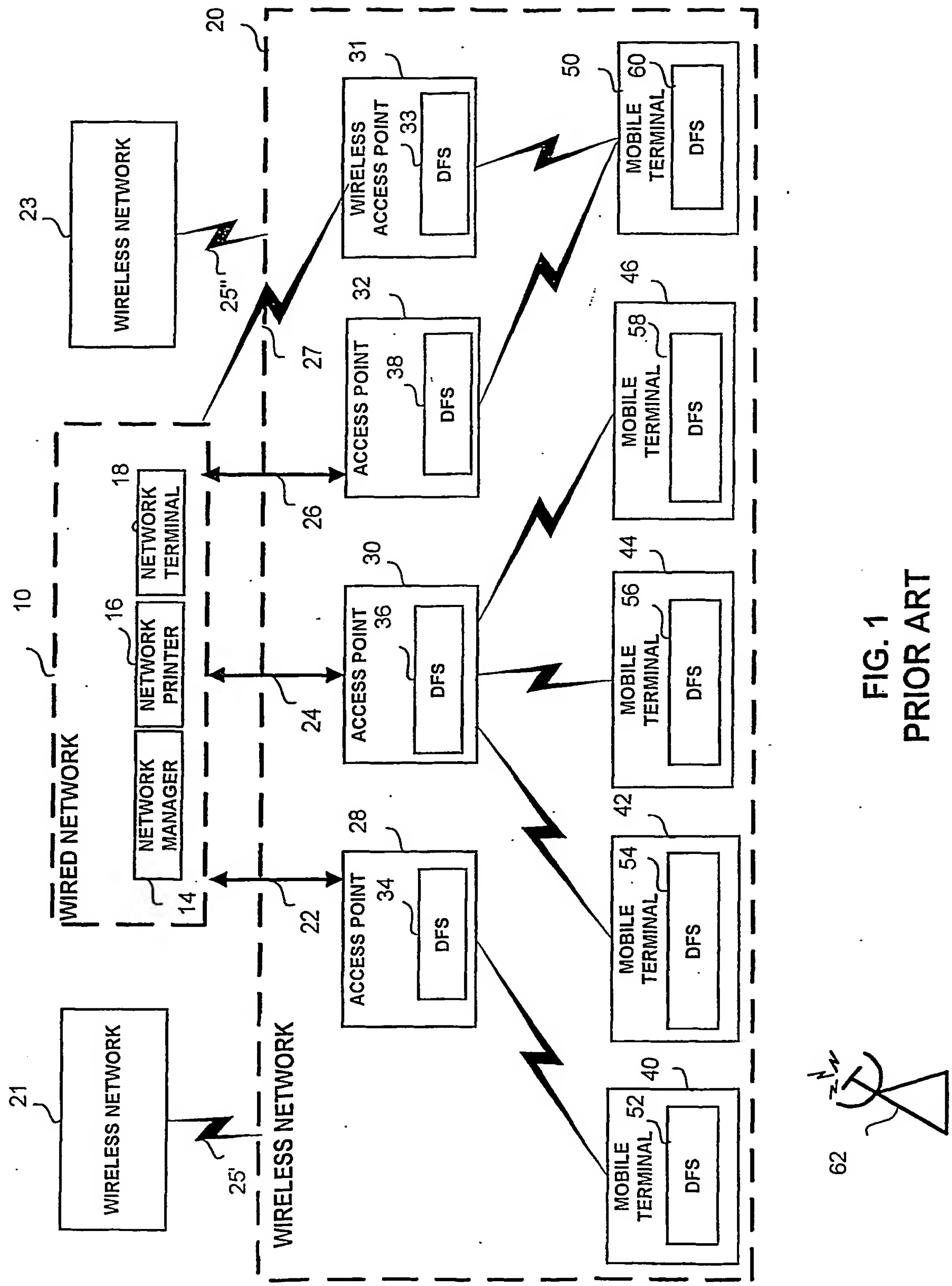


FIG. 1
PRIOR ART

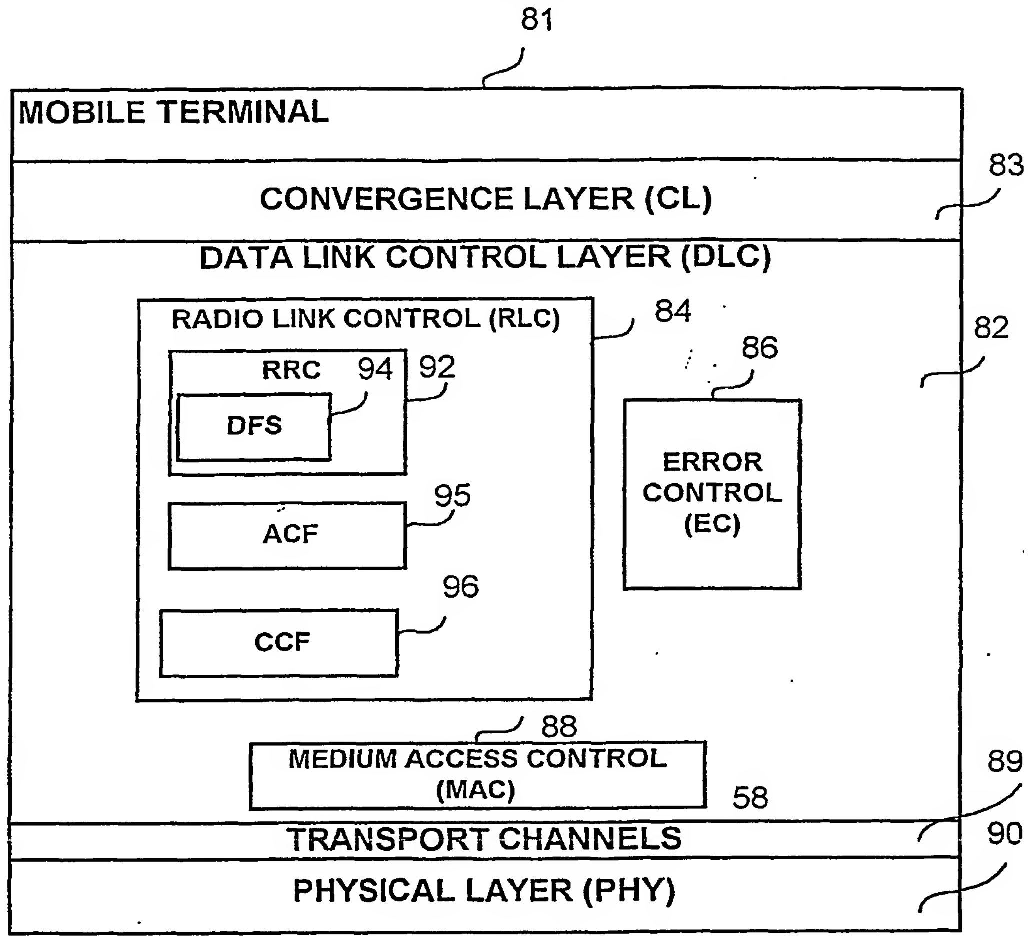


FIG. 2
PRIOR ART

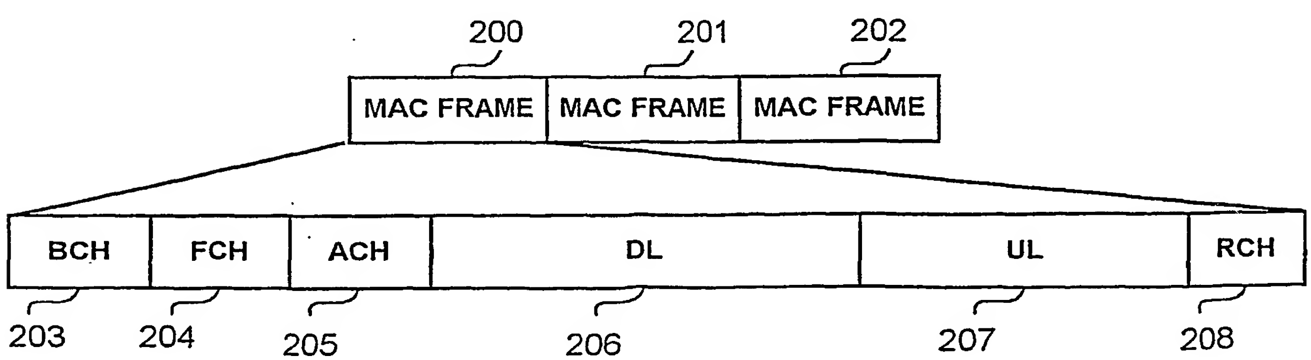


FIG. 3
PRIOR ART

3/12

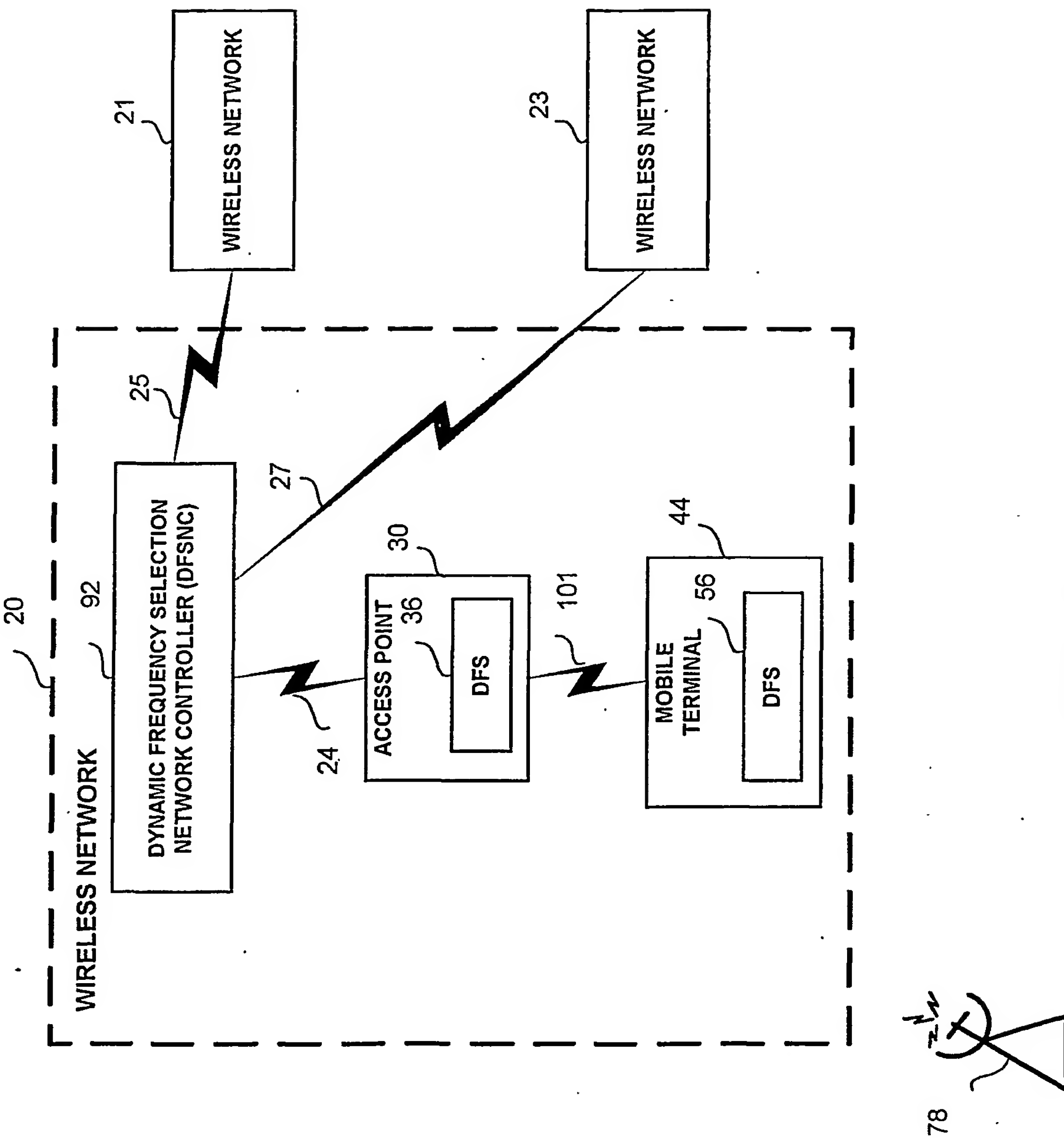
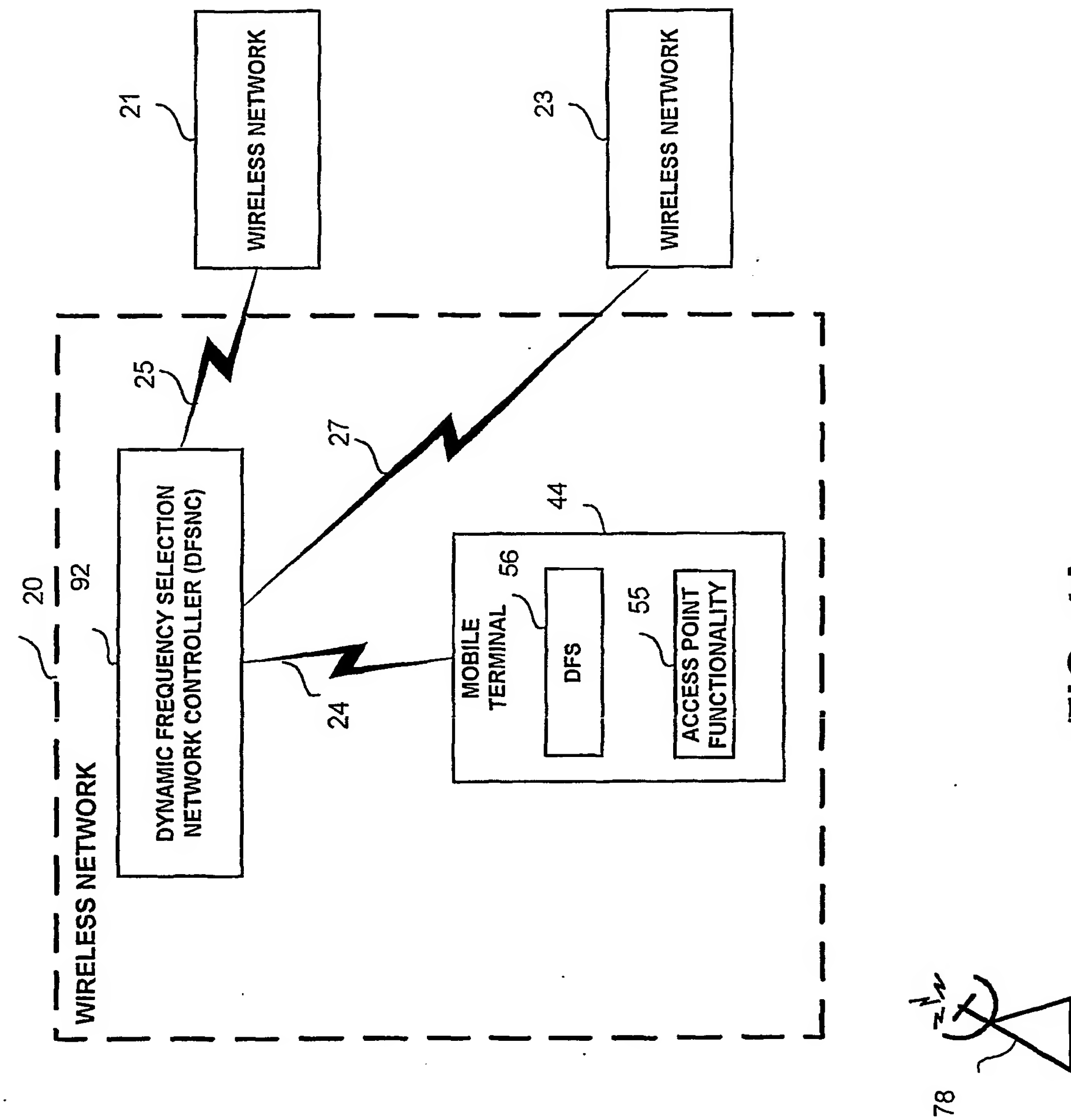

WIRELESS NETWORK
21
WIRELESS NETWORK
23
25
27
WIRELESS NETWORK
20
92
DYNAMIC FREQUENCY SELECTION NETWORK CONTROLLER (DFSNC)
24
ACCESS POINT
30
36
DFS
101
MOBILE TERMINAL
44
56
DFS
78

FIG. 4



WIRELESS NETWORK
21
WIRELESS NETWORK
23
25
27
20
92
WIRELESS NETWORK
DYNAMIC FREQUENCY SELECTION NETWORK CONTROLLER (DFSNC)
24
44
MOBILE TERMINAL
56
DFS
55
ACCESS POINT FUNCTIONALITY
78

FIG. 4A

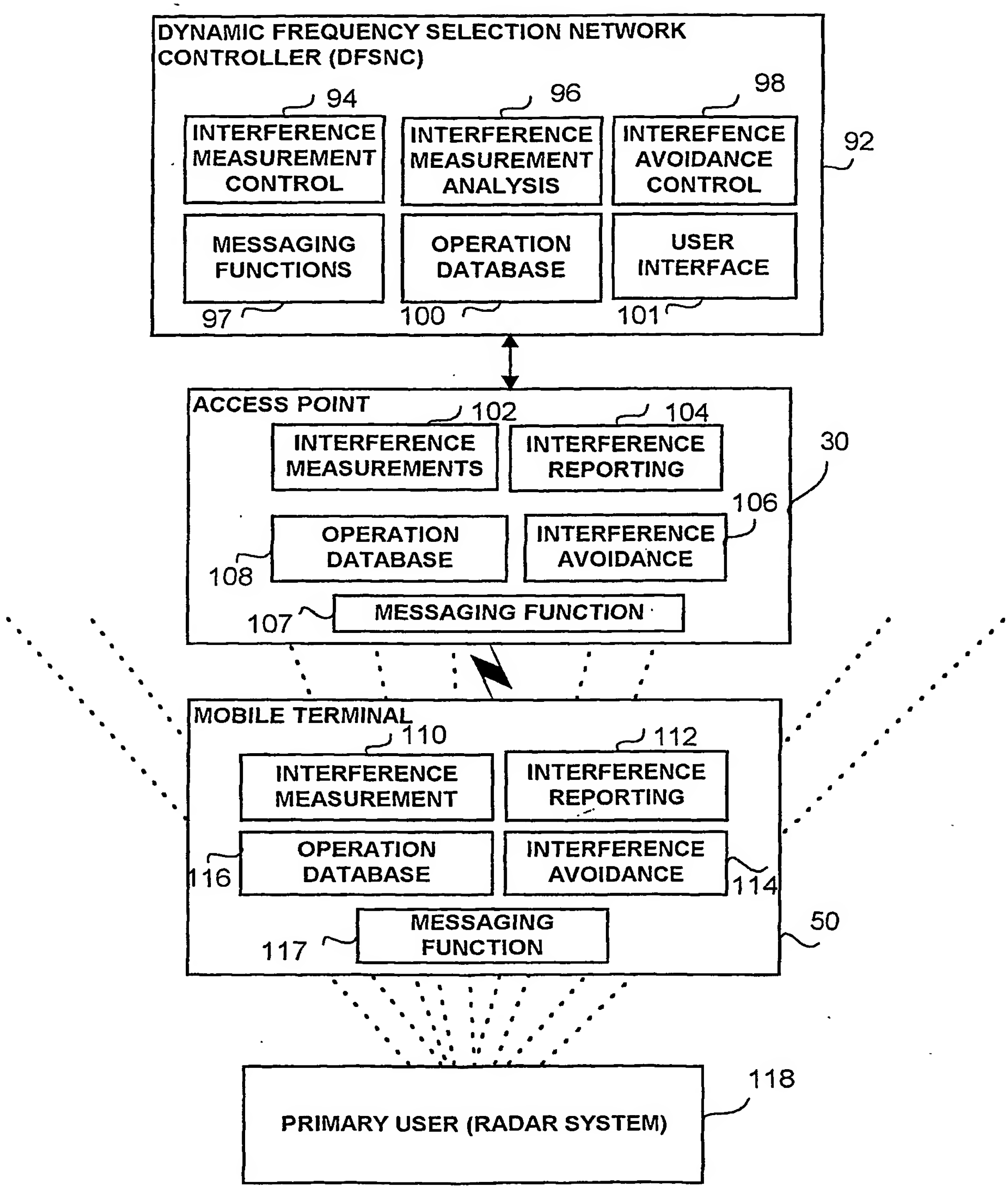
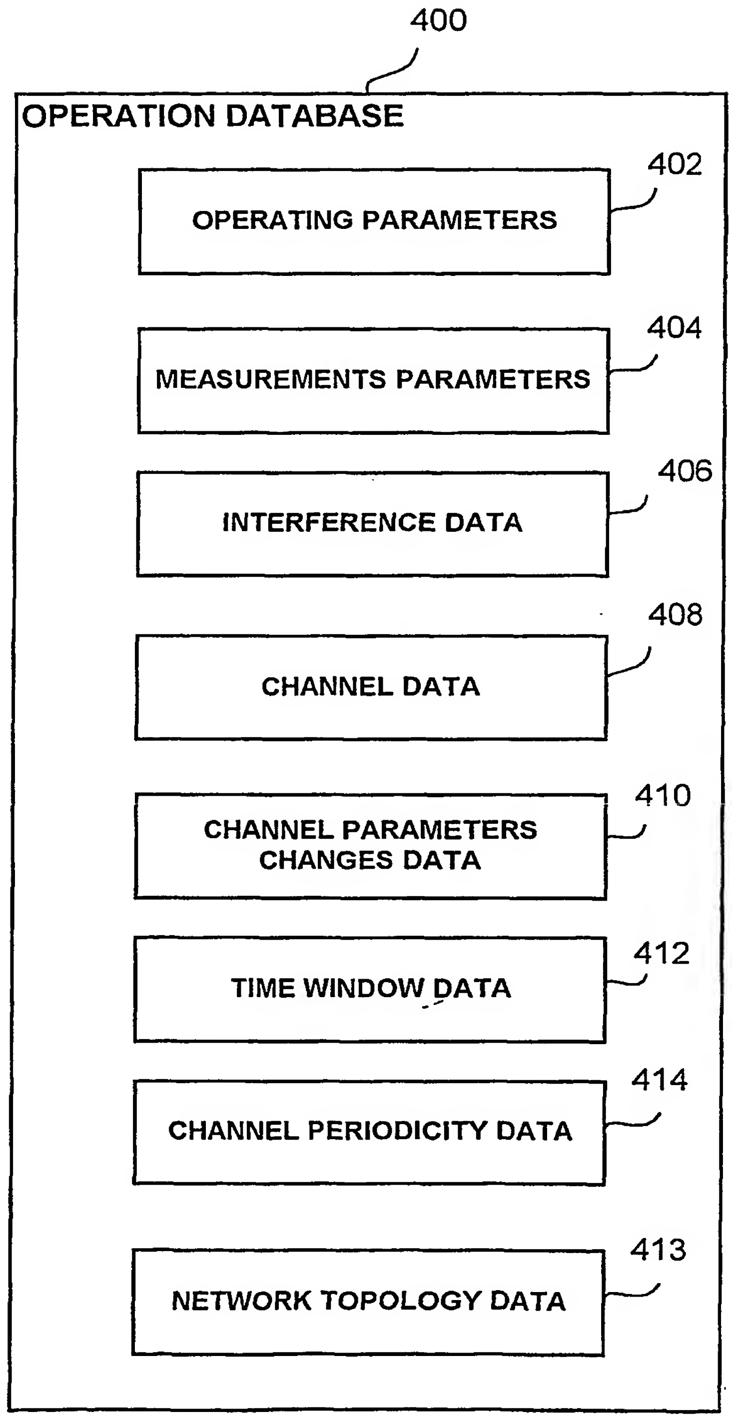

DYNAMIC FREQUENCY SELECTION NETWORK CONTROLLER (DFSNC)
94
INTERFERENCE MEASUREMENT CONTROL
96
INTERFERENCE MEASUREMENT ANALYSIS
98
INTEREFENCE AVOIDANCE CONTROL
92
MESSAGING FUNCTIONS
OPERATION DATABASE
USER INTERFACE
97
100
101
ACCESS POINT
102
104
INTERFERENCE MEASUREMENTS
INTERFERENCE REPORTING
30
106
OPERATION DATABASE
INTERFERENCE AVOIDANCE
108
107
MESSAGING FUNCTION
MOBILE TERMINAL
110
112
INTERFERENCE MEASUREMENT
INTERFERENCE REPORTING
OPERATION DATABASE
INTERFERENCE AVOIDANCE
116
114
50
117
MESSAGING FUNCTION
118
PRIMARY USER (RADAR SYSTEM)

FIG. 5



400
OPERATION DATABASE
OPERATING PARAMETERS
402
MEASUREMENTS PARAMETERS
404
INTERFERENCE DATA
406
CHANNEL DATA
408
CHANNEL PARAMETERS CHANGES DATA
410
TIME WINDOW DATA
412
CHANNEL PERIODICITY DATA
414
NETWORK TOPOLOGY DATA
413

FIG. 6

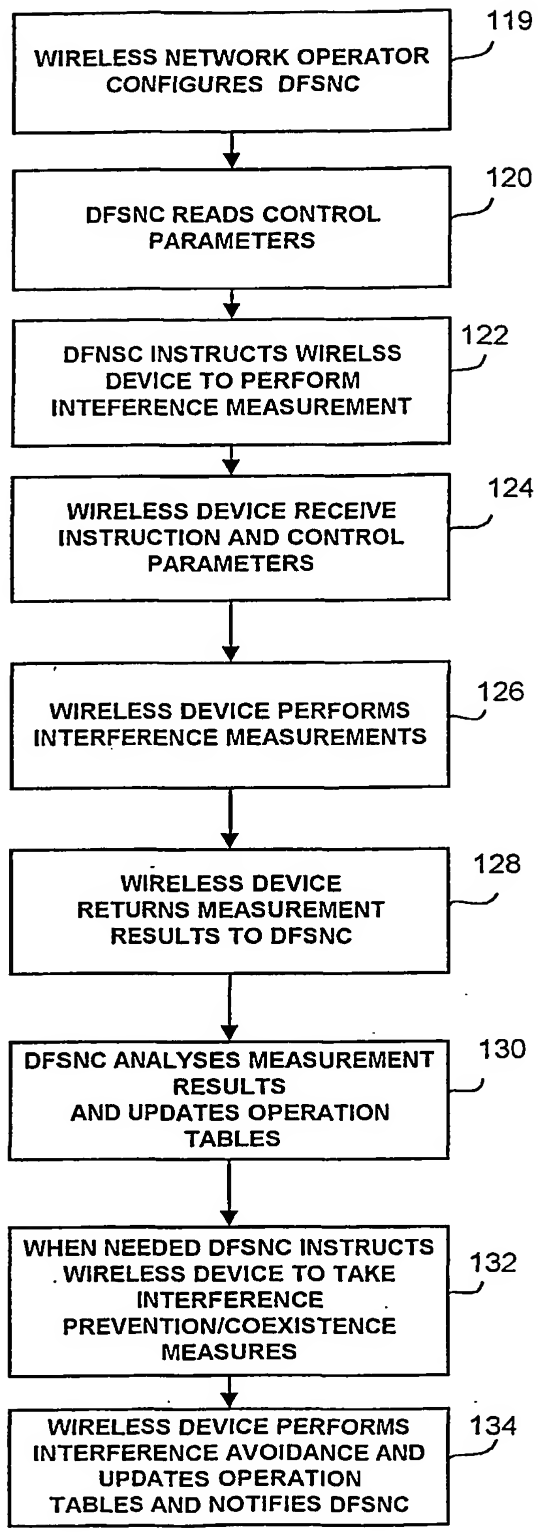

WIRELESS NETWORK OPERATOR CONFIGURES DFSNC
119
DFSNC READS CONTROL PARAMETERS
120
DFNSC INSTRUCTS WIRELSS DEVICE TO PERFORM INTEFERENCE MEASUREMENT
122
WIRELESS DEVICE RECEIVE INSTRUCTION AND CONTROL PARAMETERS
124
WIRELESS DEVICE PERFORMS INTERFERENCE MEASUREMENTS
126
WIRELESS DEVICE RETURNS MEASUREMENT RESULTS TO DFSNC
128
DFSNC ANALYSES MEASUREMENT RESULTS AND UPDATES OPERATION TABLES
130
WHEN NEEDED DFSNC INSTRUCTS WIRELESS DEVICE TO TAKE INTERFERENCE PREVENTION/COEXISTENCE MEASURES
132
WIRELESS DEVICE PERFORMS INTERFERENCE AVOIDANCE AND UPDATES OPERATION TABLES AND NOTIFIES DFSNC
134

FIG. 7

8/12

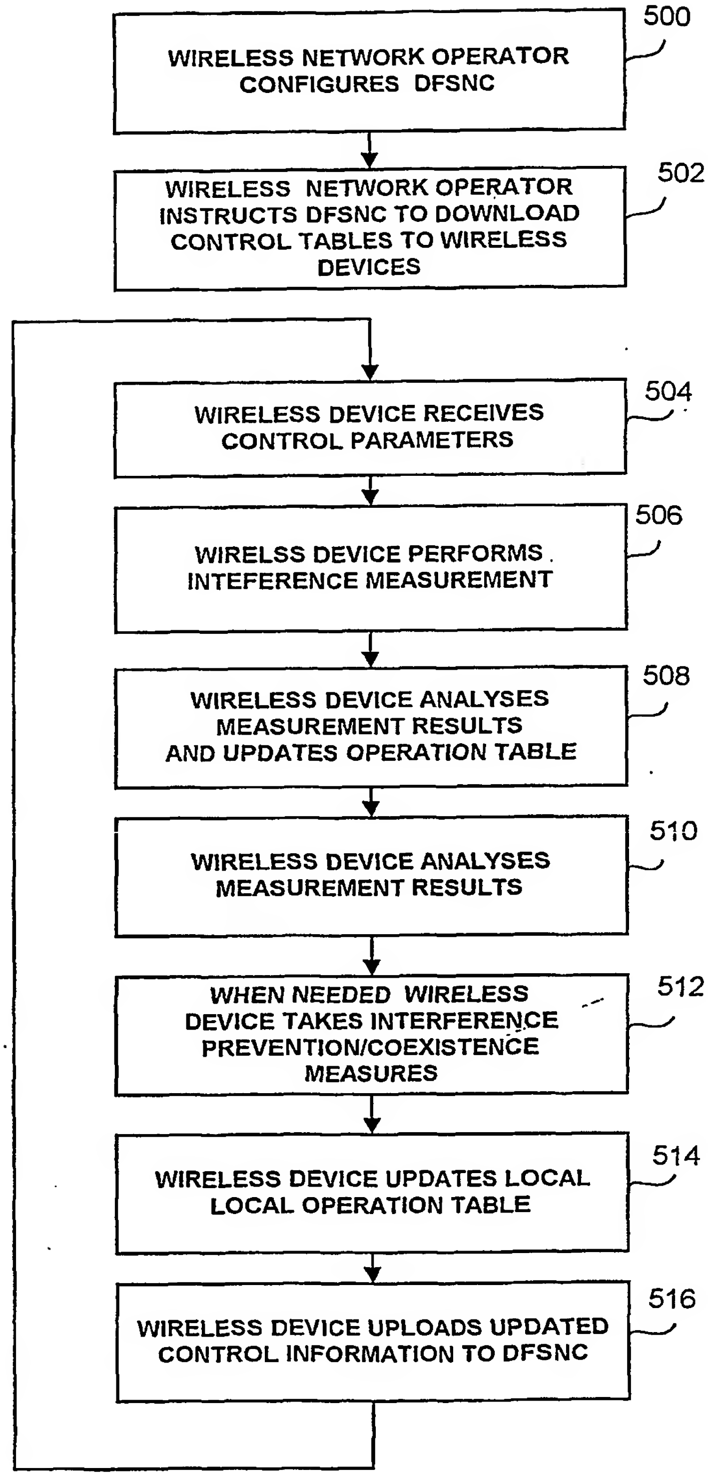

WIRELESS NETWORK OPERATOR CONFIGURES DFSNC
500
WIRELESS NETWORK OPERATOR INSTRUCTS DFSNC TO DOWNLOAD CONTROL TABLES TO WIRELESS DEVICES
502
WIRELESS DEVICE RECEIVES CONTROL PARAMETERS
504
WIRELSS DEVICE PERFORMS INTEFERENCE MEASUREMENT
506
WIRELESS DEVICE ANALYSES MEASUREMENT RESULTS AND UPDATES OPERATION TABLE
508
WIRELESS DEVICE ANALYSES MEASUREMENT RESULTS
510
WHEN NEEDED WIRELESS DEVICE TAKES INTERFERENCE PREVENTION/COEXISTENCE MEASURES
512
WIRELESS DEVICE UPDATES LOCAL LOCAL OPERATION TABLE
514
WIRELESS DEVICE UPLOADS UPDATED CONTROL INFORMATION TO DFSNC
516

FIG. 8

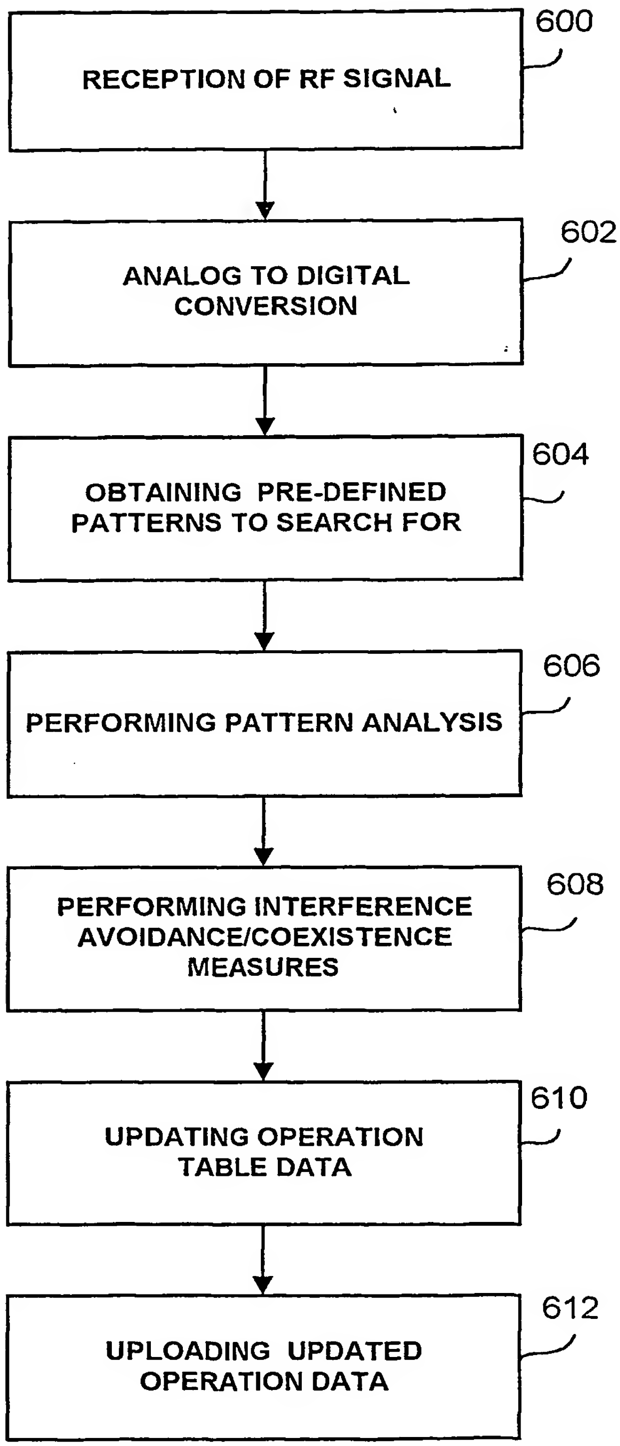
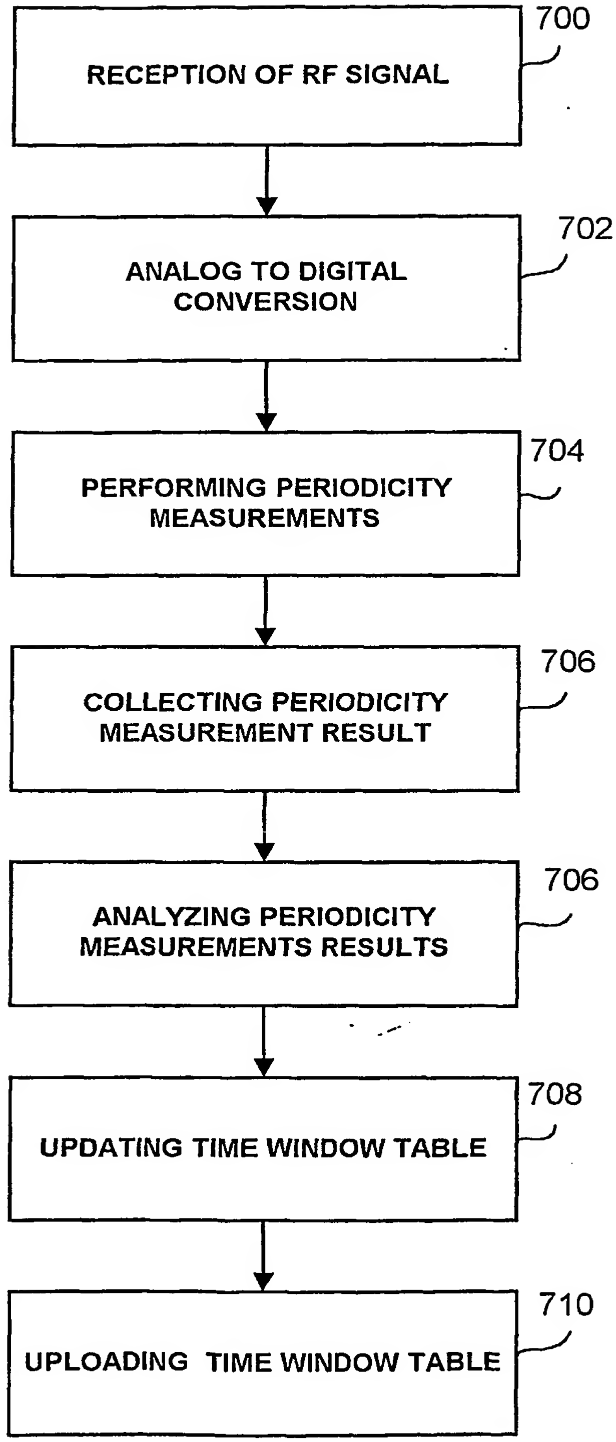
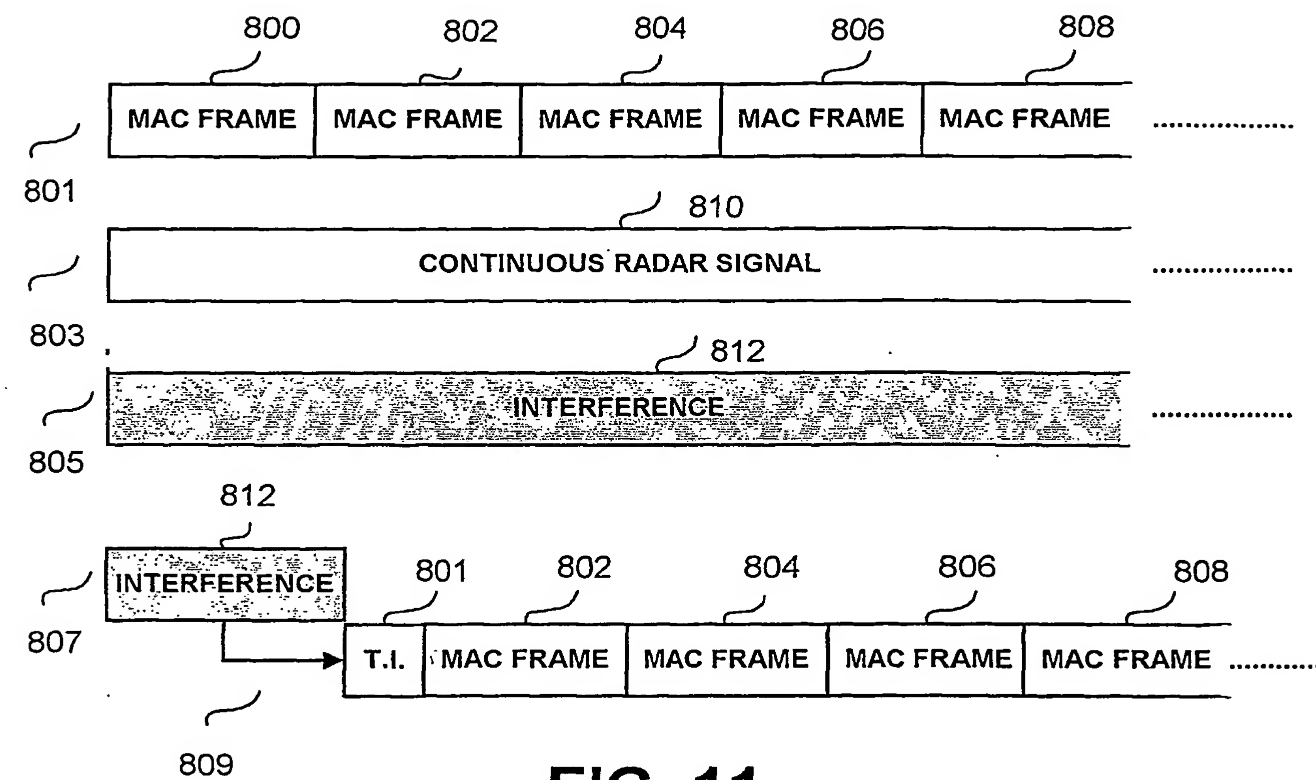

RECEPTION OF RF SIGNAL
600
ANALOG TO DIGITAL CONVERSION
602
OBTAINING PRE-DEFINED PATTERNS TO SEARCH FOR
604
PERFORMING PATTERN ANALYSIS
606
PERFORMING INTERFERENCE AVOIDANCE/COEXISTENCE MEASURES
608
UPDATING OPERATION TABLE DATA
610
UPLOADING UPDATED OPERATION DATA
612

FIG. 9



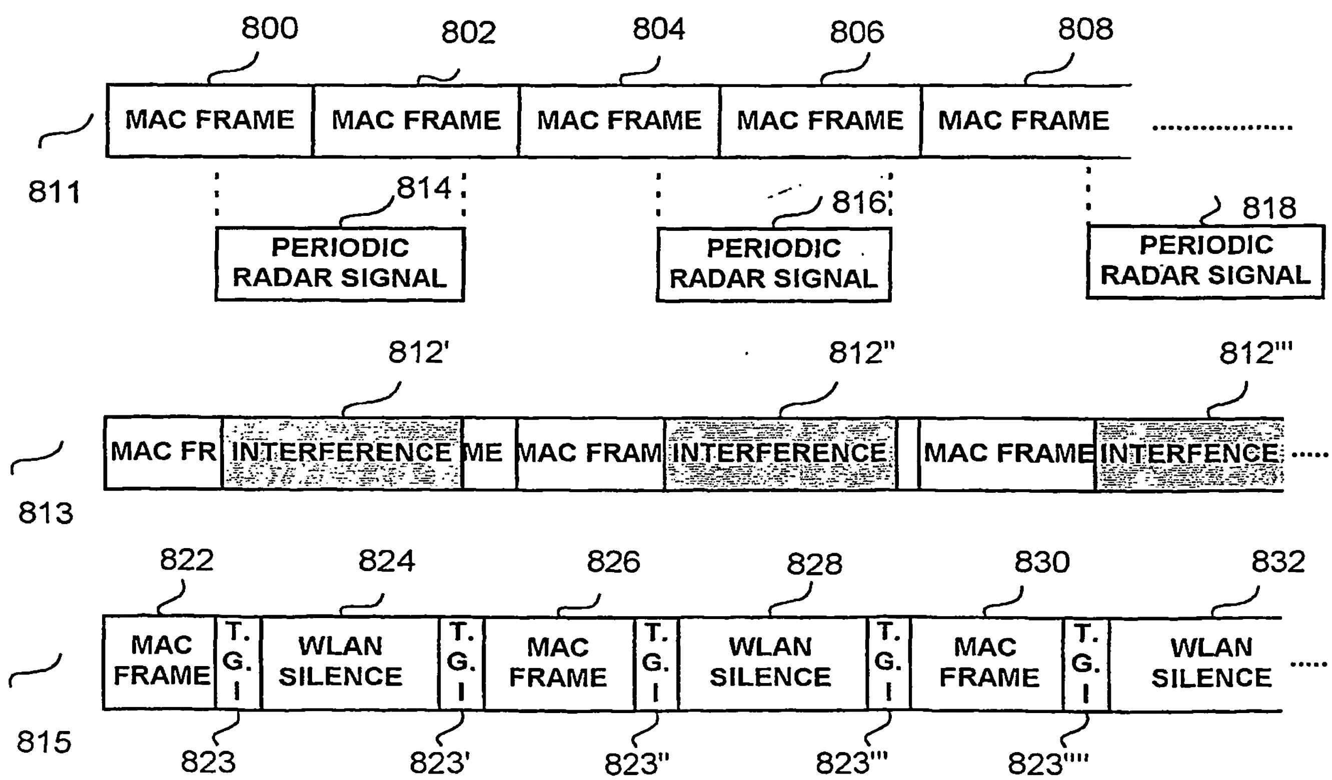
RECEPTION OF RF SIGNAL
700
ANALOG TO DIGITAL CONVERSION
702
PERFORMING PERIODICITY MEASUREMENTS
704
COLLECTING PERIODICITY MEASUREMENT RESULT
706
ANALYZING PERIODICITY MEASUREMENTS RESULTS
706
UPDATING TIME WINDOW TABLE
708
UPLOADING TIME WINDOW TABLE
710

FIG. 10



800
802
804
806
808
MAC FRAME
MAC FRAME
MAC FRAME
MAC FRAME
MAC FRAME
801
810
CONTINUOUS RADAR SIGNAL
803
812
INTERFERENCE
805
812
INTERFERENCE
807
801
802
804
806
808
T.I.
MAC FRAME
MAC FRAME
MAC FRAME
MAC FRAME
809

FIG. 11



800
802
804
806
808
MAC FRAME
MAC FRAME
MAC FRAME
MAC FRAME
MAC FRAME
811
814
PERIODIC RADAR SIGNAL
816
PERIODIC RADAR SIGNAL
818
PERIODIC RADAR SIGNAL
812'
812"
812'''
MAC FR
INTERFERENCE
ME
MAC FRAM
INTERFERENCE
MAC FRAME
INTERFENCE
813
822
824
826
828
830
832
MAC FRAME
T. G. I
WLAN SILENCE
T. G. I
MAC FRAME
T. G. I
WLAN SILENCE
T. G. I
MAC FRAME
T. G. I
WLAN SILENCE
815
823
823'
823"
823'''
823''''

FIG. 12

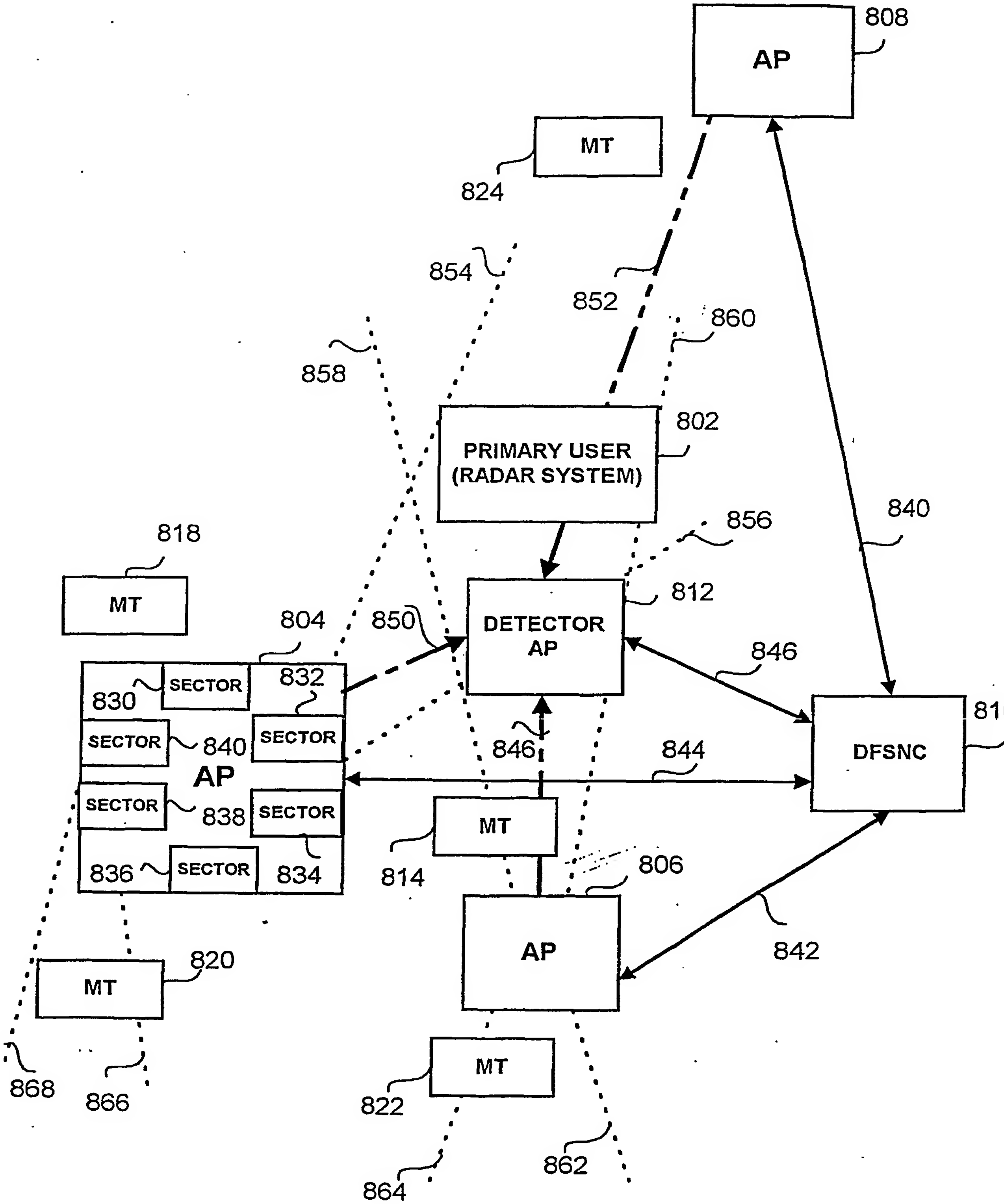

AP
808
MT
824
854
852
860
858
PRIMARY USER
(RADAR SYSTEM)
802
856
840
818
MT
812
DETECTOR
AP
804
850
846
SECTOR
832
830
SECTOR
SECTOR
840
AP
846
844
810
DFSNC
SECTOR
838
SECTOR
MT
836
SECTOR
834
814
806
AP
842
MT
820
868
866
MT
822
862
864

FIG. 13

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IL 01/00577

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 37463 A (NOKIA CORP ;SALOKANNEL JUHA (FI); LAPPETELAEINEN ANTTI (FI); SMOLA) 25 May 2001 (2001-05-25) page 5, line 4 -page 8, line 6 page 10, line 5 - line 25	1-9,11, 14-60
Y	page 14, line 6 -page 16, line 2	10,12,13
X	WO 00 70812 A (NOKIA CORP ;LAPPETELAEINEN ANTTI (FI); SMOLANDER VISA TAPIO (FI)) 23 November 2000 (2000-11-23) page 14, line 7 -page 15, line 20 figure 2	11,40
Y	WO 01 24455 A (MOBILIAN CORP) 5 April 2001 (2001-04-05) abstract	10,12,13

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 February 2002	01/03/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Schneider, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IL 01/00577

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	"Broadband Radio Access Networks (BRAN);HIPERLAN Type 2; System Overview" , ETSI TR 101 683 V1.1.1, XX, XX, PAGE(S) 1-20 XP002176358 -----	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IL 01/00577

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0137463 A	25-05-2001	FI 992473 A	19-05-2001
		AU 1527401 A	30-05-2001
		WO 0137463 A1	25-05-2001
WO 0070812 A	23-11-2000	FI 991102 A	13-11-2000
		FI 991240 A	13-11-2000
		AU 4570800 A	05-12-2000
		EP 1177652 A1	06-02-2002
		WO 0070812 A1	23-11-2000
WO 0124455 A	05-04-2001	AU 7622200 A	30-04-2001
		AU 7734300 A	30-04-2001
		AU 7734400 A	30-04-2001
		AU 7734500 A	30-04-2001
		AU 7736800 A	30-04-2001
		WO 0124454 A1	05-04-2001
		WO 0124455 A1	05-04-2001
		WO 0124456 A1	05-04-2001
		WO 0124457 A1	05-04-2001
		WO 0124458 A1	05-04-2001
		AU 7736600 A	06-06-2001
		WO 0135578 A1	17-05-2001